

Ж У Р Н А Л   К О М П Ь Ю Т Е Р Н Ы Х   Х У Л И Г А Н О В
ХАКЕР
ver. 09.01 (33)
W W W . X A K E P . R U
ХАЛЯВНЫЙ
трафик в домашних сетях
20 советов
по созданию настоящего X-кода
Захват IRC
каналов (ver. 2)
Киберспорт в России –
новое рождение
MP3/CD плееры
Джентльменский набор хацкера
Faqультет X
(game)land
ISSN 1609-1019
9 771609 101009
09>
ERRROOOOORRRRRR!!



Каждый день я попадаю в засады. Мне неустанно напоминают, что я окружен со всех сторон. Окружен уродами. Или скотами. Они гадят у меня в подъезде, сжигают кнопки в лифте, нанося на стены скудоумные надписи, мчатся на красный свет, игнорируя запуганных пешеходов, или паркуют свои самодвижущиеся повозки в произвольном порядке прямо на единственную во дворе клумбу; они с разбега запрыгивают в набитый битком вагон метро, размазывая по стенам старушек и детишек, лузгают семечки и плюют мне под ноги в подземных переходах, а потом гуляют по заблеванным детским площадкам со своими волкодавами, держа в панике бедных детишек. Это они заставляют весь дом слушать свои убогие "Руки вверх", распивая винище в три часа ночи, обращаются ко мне со словами "Слышь, тыыыы..." и пишут мне письма, где встречаются настолько фантастические грамматические ошибки, что желание читать что-либо пропадает вообще. Они же требуют прислать "крякер интернета" и ленятся заглянуть в самые элементарные FAQ-и, предпочитая "загрузить" своими откровенно дурацкими вопросами всех вокруг, они с утра до вечера льют нам в уши всякий отстой с телеэкранов, подсаживая целые поколения на дебильных телепупзиков, гадя нам прямо в мозг вилларибскими тётеасями и распевая "под фанеру" песни, написанные либо идиотами, либо для идиотов. Их много. Они везде. Они задолбали меня своими проблемами. Знакомая ситуация?

Однажды мне это надоело. Просто как-то почувствовал, что устал жить на скотном дворе. Я решил попробовать восстановить справедливость и вернуть проблемы их законным владельцам. Начать я решил с себя самого. Это очень сложно, иногда неприятно и занудно, но поверь мне – цель достижима и стоит потраченных на нее усилий. А потом... Молодой парень, пойманный "на месте преступления", после непродолжительной беседы вытер свое дерьмо в подъезде своим же модным свитером, дворовый автолюбитель навсегда зарекся ставить свой рыдван под моими окнами после целой серии акций воспитательного западлостроения, а подросток, проживающий этажом ниже, меньше чем за шесть часов смыл со стен свои автографы. Средних лет дядя с блестящей лысиной, забежавший в вагон и как следует "запрессовавший" меня, тут же как пробка вылетел на платформу после мощного пинка и довольно быстро смекнул, что в метро перевозят людей, а не скотов. ПионЭры с их винищем и музыкой были сданы с рук на руки заспанным и злым родителям в пятом часу ночи. Судя по уважительным взглядам через недельку, отцовские ремни восстановили тягу к прекрасному у подрастающего поколения. А письма... мне кажется, что человек, приславший мне письмо с кучей ошибок, просто считает меня быдлом, способным беседовать на его родном – скотском, а не на русском языке. Ты бы с таким общался?

Не думай, что я решил загрузить тебя краснозвездными тимуровцами и пионерской романтикой. Нет, мне это не нужно. Я хочу, чтобы ты посмотрел на свою жизнь другими глазами и хотя бы попробовал что-то в ней изменить к лучшему. Иначе мы все навсегда останемся там, где пребываем сейчас. Пока ты молод и полон сил, начни с себя, задумайся о том, как все-таки выдавить из себя то скотство, которое не дает нам всем нормально жить. Если ты одержишь верх хотя бы над своим равнодушием, то наши шансы выплыть сильно возрастут. Так к чему я все это? Все просто. Пока что я один, и против армии уродов на всех фронтах мне не устоять. Один в поле не воин. Но если ты, хотя бы ты один, решишь ко мне присоединиться, нас сразу же станет двое – больше ровно в два раза. А твои и мои друзья? Вот нас уже четверо, вот четыре сотни, четыре тысячи... и все – наши!

Прости за то, что взялся тебя воспитывать. Я всего лишь искренне хочу помочь тебе. Однажды, когда ты поймешь, что твоя жизнь зависит ТОЛЬКО ОТ ТЕБЯ, она обязательно изменится. Я искренне желаю тебе, чтобы момент прозрения наступил как можно раньше, а пока что готовься: бороться с уродами будет нелегко, но у нас с тобой есть в запасе могучее "вундерваффе", и имя ему – ХАКЕР! No pasaran!

Х–Crew в лице
Синтеза
Центнера
Сайдекса
Ядовитого
Пороха
и всех остальных

editorial
/братская могила/

Редакция

самый главный редактор
Сергей "SINtez" Покровский
(sintez@real.xakep.ru)
самый дедлайновый редактор
Иван "SideX" Корноухов
(sidex@real.xakep.ru)
самый ударный редактор
Михаил "Centner" Михин
(centner@real.xakep.ru)
самый геймерский редактор
Александр "2poisonS" Сидоровский
(2poisonS@real.xakep.ru)
самый железный редактор
Константин "p0r0h" Буряков
(p0r0h@real.xakep.ru)
корректор
Виталий Петрович
(vp@gameland.ru)

Art

Арт-директор
SINtez
обложка
Кирилл Петров
дизайн верстка
Алик Вайнер (Jmurik)
(alik@real.xakep.ru)
иллюстрации
Михельсон
Алекс Кондаков
Алик Вайнер (Jmurik)

Реклама

руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
менеджеры отдела
Алексей Анисимов
(anisimov@gameland.ru)
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
тел.: **(095) 229.43.67**
(095) 229.28.32
факс: **(095) 924.96.94**

PR

PR менеджер
Михаил Михин
(pr@gameland.ru)

Оптовая продажа

руководитель отдела
Владимир Смирнов
(vladimir@gameland.ru)
менеджеры отдела
Андрей Степанов
(andrey@gameland.ru)
Самвел Анташян
(samvel@gameland.ru)
тел.: **(095) 292.39.08**
(095) 292.54.63
факс: **(095) 924.96.94**

PUBLISHING

учредитель и издатель
ЗАО "Гейм Лэнд"
директор
Дмитрий Агарунов
(dmitri@gameland.ru)
финансовый директор
Борис Скворцов
(boris@gameland.ru)

Служба безопасности и связь с правоохранительными органами
Игорь Акчурин
Глеб Маслов

Для писем
101000, Москва,
Главпочтамт,
а/я 652, Хакер

Web-Site **http://www.xakep.ru**
E-mail **magazine@xakep.ru**

Отпечатано в типографии
«**ScanWeb**», Финляндия
Зарегистрировано в Министерстве Российской Федерации
по делам печати, телерадиовещанию
и средствам массовых коммуникаций
ПИ № 77-1905 от 15 марта 2000 г.

Тираж **57 000** экземпляров. Цена договорная.

CONTENT

НЬЮСЫ

ФЕРРУМ

PC_ZONE

Х-СТИЛЬ

ВЗЛОМ

КОДИНГ

СЦЕНА

JOYSTICK

ЮНИТЫ

добро пожаловать в нашу реальность...

WARNING!!!

Редакция напоминает, что вся информация, которую мы предоставляем, рассчитана прежде всего на то, чтобы указать различным компаниям и организациям на их ошибки в системах безопасности.

Наш маленький, гаденький, мерзопакостный тест :). Пройди его и пойми кто ты. Тест получился очень точным, мы все содрали с журнала “Животноводство сегодня”, а уж там то о хакерах знают все!

стр. 54





проги – это не только наши релизы, которые лежат на сайте. Это любой софт, который мы любим, юзали, юзаем и будем юзать. Сканнеры, hex-редакторы, трейсеры и пр.: все это проги.

Вот и разродились мы второй версией многотомной саги о захвате каналов в IRC. Нам написал один чел, сказав, что все, что было раньше – гон, он опишет все в 2млн. раз лучше. И реально написал. Прочти, оцени творчество. На наш взгляд – отлично!

стр. 46

проги

HITECH NEWS

Алекс Целых (technews@mmub.ttn.ru)

Собачий коммуникатор

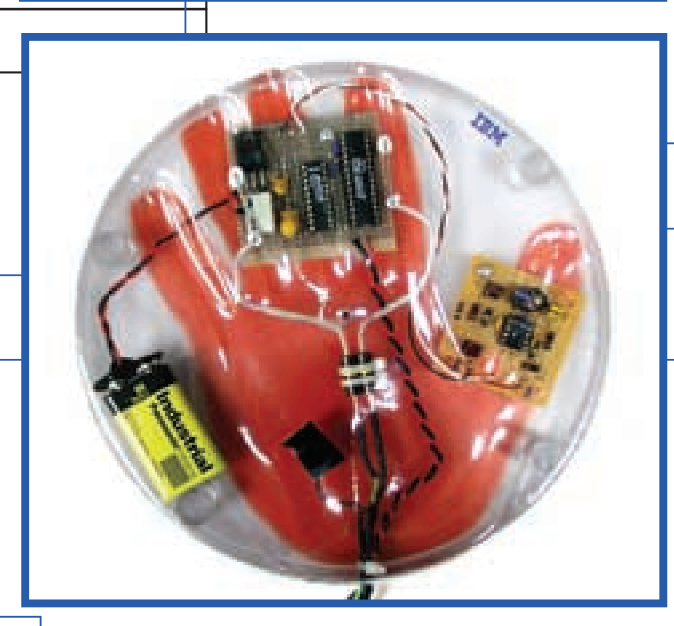
Японская компания Takara (www.takara.co.jp) разработала коммуникатор для собак.
Устройство переводит собачий лай на человеческий язык и помогает хозяевам лучше чувствовать переживания питомца. Для этого на ошейник крепится небольшой микрофон весом 60 граммов. Через инфракрасный порт "речь" собаки транслируется на пульт управления, где и озвучивается. Одновременно на жидкокристаллическом экране появляется фраза "я раздражена" или "как мне весело", "пора обедать", а под ней - мохнатая мордашка с соответствующей миной. В словаре устройства 200 слов и эмоций. Рык, вой, собачье посапывание соответствуют чувству угрозы, скуке, радости, печали. А вечером коммуникатор составляет подробный отчет о настроении пса за день. Выглядит это как душещипательный рассказ от первого лица. Новинка появится в магазинах уже в будущем феврале по цене не дороже 100 долларов.

Жилетка хай-тек

Чикагский адвокат продает модные хай-тек жилетки.
Перец устал распихивать по карманам электронное добро: сотовый телефон, карманный компьютер, наушники, батарейки и складную клавиатуру. Подумав, он изобрел жилет (scottevest.com) с 15-ю карманами, в котором все это дело не только "хорошо лежит", но и слаженно работает. Причем, провода не болтаются на шее и совсем незаметны для окружающих. В продольных планках, закрытых клапанами на липучках, проделаны отверстия. Через них и прокладываются провода, например, от наушников к MP3-плееру или от сотового телефона к карманному компьютеру. Кроме того, в жилете куча наворотов: от прищепки для ключей до специальных мягких карманов для очков. Жилет хорошо передает вибрацию сотового телефона, а несколько отделений имеют двойное дно - чтобы устройства не соприкасались друг с другом. И вообще, это редкий пример хай-тек одежды, отвечающей запросам моды. Продается по цене 159 долларов.

Мышь-психопатка

Инженеры IBM разработали новую модификацию психоделической компьютерной мыши.
"Эмоциональная мышь" (Emotion Mouse II) чувствует настроение хозяина и с успехом под него подстраивается. Новинка представляет собой конструкцию неожиданно круглой формы с углублением по рисунку ладони. Внутри установлены инфракрасные, гальванические, механические и прочие сенсоры. Они измеряют пульс, температуру, проводимость кожи, дрожание рук. Если хозяин чем-то взволнован, мышь делает все возможное для снятия стресса. Умный грызун включает шум водопада, предлагает сделать паузу в работе или мило шалит.



Нарисованные рельсы

В Голландии испытывают новый трамвай, двигающийся по нарисованным путям.
Виртуальные рельсы нанесены на асфальт при помощи специальной магнитной краски. Камера на днище трамвая точно следит за изгибами цветной полосы. При малейшем отклонении от маршрута в бортовой компьютер вводится поправка. Вероятность схождения с виртуальных рельс практически равна нулю, в отличие от обычных трамваев. А чтобы перенести такой маршрут, достаточно снова взять в руки кисть и перевесить высоковольтные провода. К 2003 году новые трамваи будут колесить по улицам американского Лас-Вегаса, а позже появятся и в других странах.

Кровавое" кресло

Американская компания Baxter (www.baxter.com) разработала хай-тек кресло для доноров.
Процедура сдачи крови обычно длится от 10 минут до 2 часов. Все это время доноры страдают от безделья и не знают, чем заняться. С новинкой от Baxter они получили возможность браузить Интернет, читать почту и смотреть блокбастеры. В кресло встроен компьютер с выходом в Сеть, DVD-плейер и стереонаушники. По словам разработчиков, пользоваться благами цивилизации смогут также больные, которым предписаны длительные медицинские процедуры вроде очищения крови и химиотерапии. Завоз хай-тек кресел в американские клиники намечен на ближайшие месяцы.

"Зубастики"

Инженеры компании Panasonic сконструировали зубную щетку со встроенной видеокамерой.

Миниатюрная камера уместилась между вибрирующими щетинками электрощетки. Изображение с нее передается на телевизионный экран, что позволяет владельцу отчетливо наблюдать невычищенные кусочки пищи в собственных зубах. Теперь заниматься полезным делом можно не вслепую, как это до сих пор происходило, а полностью отдавая себе отчет в том, что делаешь.

Костюм супермена

Японские ученые изобрели робокостюм для поднятия тяжелых грузов, превышающих вес человека.

Устройство представляет собой металлический каркас с пятью пневматическими приводами: по одному для каждого локтя и колена и один на поясницу. Приводы приходят в движение по сигналу микрокомпьютера, считывающего данные о давлении на пластинки-датчики на всех основных группах мышц. Первыми костюм оденут медсестры и физиотерапевты, так они смогут поднимать с кровати пациентов, не прилагая ощутимых усилий. Во время испытаний хрупкая медсестра держала над своей головой пациента, весившего 70 килограммов.

Пока что костюм не отличается практичностью. Прототип весит 16 килограммов, а одетому в него человеку приходится таскать за собой путаницу проводов и шлангов, по которым поступает сжатый воздух. Цена на устройство достигает 21 тысячи долларов. Однако, по словам ученых, совсем скоро машина станет легче и удобнее. Уже через пару лет переодеться в супермена можно будет за 200-300 буказоидов.

Белгород впереди планеты всей

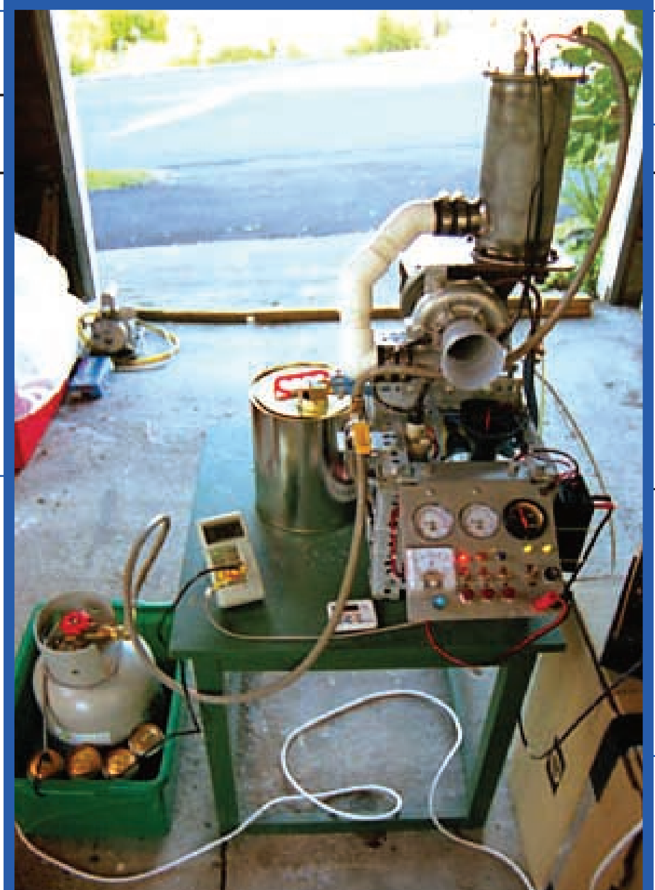
12 августа сего года в российском городе Белгород группа энтузиастов взяла и широко отпраздновала знаменательную для многих дату: 20 лет с момента появления первого персонального компьютера IBM PC. Большое спасибо организаторам праздника: белгородским компьютерным компаниям "КИТ" (www.citcompany.ru) и "Бизнес и АРТ" за замечательную идею и не менее замечательную реализацию. На праздник собрались все самые просвещённые белгородцы, которые, к огромному удивлению организаторов, проявили завидную осведомлённость в компьютерных и околокомпьютерных вопросах. И совершенно не зря, ведь всем, правильно ответившим на каверзные вопросы, вручались призы, главным из которых был процессор P4 и материнская плата под него.

Самый положительный момент в организации праздника - его доступность и отсутствие скучного официоза. Мы очень надеемся, что с течением времени праздник обретёт статус общегородского и вырастет в настоящее, масштабное мероприятие, которому сможет позавидовать даже "Комтек". Журнал "Хакер" обязательно поддержит следующий компьютерный праздник в Белгороде. Подробности о проведении праздника можно найти на его официальном сайте www.peacepc.csn.ru

Хай-тек скамейка

В английском графстве Саффолк к Интернету подключили главную городскую скамейку.
В каждую ручку деревянной “сидушки” встроили по две телефонные розетки, итого четыре. Даже при сильном желании больше чем четверо на скамейке не поместятся. Теперь любой, у кого есть ноутбук, может выйти в Интернет через местного провайдера. Первые три месяца телефонные счета, в порядке эксперимента, оплачивает спонсор проекта, Microsoft. Этим фактом не замедлили воспользоваться двое местных перцев. Оказалось, что через штекер скамейки можно подключить обычную трубку. А баг позволяет звонить по межгороду. Перцы дозвонились секретарю Гейтса в Штатах, и “лавочку” прикрыли.





Холодное пиво

Житель Новой Зеландии построил охладитель пива на реактивной тяге. В основу изобретения лег известный физический закон: при расходовании топлива из баллона со сжиженным газом его корпус сильно охлаждается. Абориген поместил в емкость с водой упаковку любимого пива “Гиннес” и собрал реактивный двигатель на основе автомобильного турбокомпрессора. Двигатель делает 100 тысяч оборотов в минуту и издает шум в 125 децибел (взлетающий реактивный истребитель). По словам этого Эйнштейна, пяти минут работы устройства хватает на то, чтобы охладить несколько банок пива с +14 до +2 градуса Цельсия. На странице проекта (asciimation.co.nz/beer/) изобретатель настойчиво просит не повторять эксперимент: “Пиво - очень опасная жидкость, когда используется без должного внимания!”

“Чемодан на поводке

Английский ученый изобрел самоходный чемодан.
Умный саквояж на колесах везде следует за своим хозяином, ориентируясь на сигнал радиопередатчика в его кармане. На тот случай, если рядом окажутся несколько кейсов, устройство излучает код уникальной частоты. “Услышав” владельца, чемодан идет за ним след в след по проложенному пути, стараясь не отставать. Если неожиданно возникает преграда или садится аккумулятор, саквояж подает сигнал бедствия.

Электрическая мухобойка

Канадская Компания Triwin (www.triwin.com) продает электрические мухобойки.
Устройство, с виду напоминающее яйцерезку, позиционируется как очень эффективное и экологически чистое средство борьбы с насекомыми. Согласно прилагаемой инструкции, обнаружив вредителя, нужно пустить пробную искру и слегка коснуться крылышек “атакующей поверхностью”. Электрическим разрядом насекомое будет сражено наповал и опрокинется кверху лапками, не запачкав обоев. В списке “личных врагов” мухобойки: комары, муравьи, термиты и даже клопы. Продуманная конструкция устройства позволяет вести охоту не только на открытой поверхности, но и по углам и даже в воздухе. Новинка питается от 4 пальчиковых батареек и продается по цене 40 долларов.



Сам себе батарейка

Вице-президент США заряжает свой мобильник во время оздоровительной гимнастики.

Устройство Pedal and Power (ikonglobal.com), полученное Диком Чейни в подарок от английского изобретателя, превратило велотренажер вице-президента в динамо-машину с педальным приводом. Регулярные физические упражнения чиновника теперь ко всему прочему помогают сохранить окружающую среду. Pedal and Power с разъемом для подключения мобилы любой марки можно купить за 38 долларов.

Робот-костолом

Игровой автомат поломал гонконгских армрестлеров.

Проблемы в парке аттракционов Гонконга начались с появлением там новейшей силовой установки для армрестлинга. Диковинный автомат полностью управляется компьютером. Каждый раз машина честно предупреждает соперника о возможных негативных последствиях и предлагает фору. Однако то ли пострадавшие совсем не рубили в английском, то ли национальная гордость взыграла - все выбирали сложнейший режим. В итоге, пять человек обратились к врачам с переломами рук.

Без ног - с ушами

В Японии создан безногий робот, который все-все слышит.

Робот Sig не имеет ног и рук, зато у него отменный слух и горячее желание служить людям. Слуховая система робота - точная копия человеческой. Уши расположены по бокам головы. Как известно, наличие двух точек восприятия звуковых волн позволяет людям быстро находить источник звука. При помощи глаз-видеокамер робот внимательно следит за собеседником, всегда оставаясь к нему лицом. Впрочем, самой главной особенностью робота является его умение распознавать речь в шумной обстановке - например, на улице или в комнате, наполненной людьми. По словам разработчиков, Sig легко справится с работой портье в гостинице или оператора в справочном бюро.

Triple Action

Новый удар Мобильного фестиваля Новой Культуры «Катапульта» наблюдался 9 августа сего года в клубе «Б-2». С двух часов дня в клуб стали подтягиваться ряды музыкантов, для проведения саундчека, чтобы вечером все присутствующие смогли насладиться стройностью звучания, как монстров, так и начинающих талантов музыкального Олимпа. А на специально подготовленной площадке перед сценой клуба разминали свои конечности представители Лиги брейкдансеров России. Пройдя по витиеватому деревянному коридору, разрисованному граффити, и преодолев три этажа ступенек, физически и морально подготовленные к заряду адреналина гости попадали к месту событий. На сцене и в кулуарах были замечены представители следующих ВИА и народных коллективов: «Братья Улыбайте», «Лед за полем», «Net Dela», «Агония», «Флюиды», «Тотал», «IFK» и независимый Артемий Троицкий.

Этой акцией Мобильный фестиваль Новой культуры «Катапульта» завершил свой летний клубный тур, но фестиваль продолжается, следи за www.catapulta.ru.

BUGTRAQ

COMPOSED BY RAW POWER (FAQ@REAL.XAKEP.RU)

Store.cgi
by _TacK_ (TacK@ole.com)
Скрипты гостевух, системы новостей и онлайн-шопы – самые лакомые кусочки, доступные для разделки хакеру. Результат полома разный – от примитивного редактирования форума до взятия полного контроля над сервером, а то и всего окружения машин. Уязвимая корзинка на серванте даст мазу захвата "всего-навсего" базы CC, прошедших транзакцию. Неплохая находка, неправда ли? Данный баг позволит зачитать любое доступное файло на сервере. Многие возмутятся, что с данной дыркой шадов или конфиги апача утянуть чаще всего не удастся. А нам этого и не надо! Т.к. чтение свопа CC-движка обычно доступно через бажную корзину. Итак, берем в кулак store.cgi. http://www.xakep.ru/cgi-bin/Store/store.cgi?product=../../../../../../../../../etc/passwd%00
Как видишь, поломка производится радикально просто – добавлением небольшой кучки /../ после переменной product (=) В итоге стягиваем любой файл системы. Главным образом – базу номеров. Здесь можно утянуть сорцы корзины + обнаружить списочек ее юзеров (прямая наводка кого ломать ;) – *http://www.keyweb.com.*

Windows 2000 IRDA Driver
by Paul Millar (paulm@astro.gla.ac.uk)
Всякий раз, активируя инфракрасный порт на своей Nokia 6210, я задумываюсь о секьюрности этого: а не перехватят ли таким образом мою записнуху, своп SMS-сообщений и другое? Пока все в порядке. Но IR встречается не только в мобилах и пультах от телевизора, в данном случае баг обнаружился в софте Win2K, заточенном на работу с инфракрасными девайсами. Баг – переполнение буфера в драйвере, обеспечивающем поддержку IRDA-протокола. Что же получается хорошего с дыры? Мы можем направлять левые пакеты в систему рассматриваемым путем. Стартануть исполняемый код не удастся, зато направить систему в ребут – окажется плевым делом. Предполагается, что машина атакующего должна находиться в непосредственной близости от жертвы для участия в IR-потоке. Дополнительная инфа в бюллетене от MS – *http://www.microsoft.com/technet/security/bulletin/ms01-046.asp.*

Lotus Domino mail server
by Ian Gulliver < ian@orbz.org >
Как-то ко мне обратился чел с просьбой добыть варезом ряд продуктов Лотуса. К чему оно ему было? Большинство работ рассматриваемой конторы имеет бесплатные аналоги. Но многих прельщает качественный саппорт, регулярные обновления... стереотипы опять же подавляют логику. Но, как показала практика, security-саппорт оказался не силен: новый баг является массивной тенью предыдущего, случившегося фактически дважды – в мае этого года и марте предыдущего. Коммерческие продукты обычно инсталлируют на мощные сервера. Но установившие Домино потеряют всяческую мощь путем 100% прогруза проца. Как? Отправляем письмо, вроде такого:
MAIL FROM:<bounce@[127.0.0.1]>
RCPT TO:<address@domain.com>
Фишка в том, что domain.com не относится к серверу получателя, и сервак, естественно, попытается вернуть письмо отправителю, но попадет на всем знакомый loop, т.е. войдет в петлю и достаточно быстро сожрет все 100% ресурсов системы. Баг протестирован на Lotus Domino R4.63, R5.01, R5.05 и R5.08. Официального патча пока не было, и единственным решением остается – перезапуск системы, удаление злополучного письма, перезапуск почтовика. Но это не станет капитальным решением трабла, т.к. в случае следующего получения заподлянного письма – глюк повторится.

Sendmail
Cade Cairns <cairnsc@securityfocus.com>
На мой взгляд, использование сендмыла админом, который знает о существование Postfix`а и qmail`а, – нелогично. Первая тема о степени security сервака – наличие suid`ных прог на нем. Первой же проблемой часто оказывается требование sendmail`ом – root привилегий. Новый баг – локальный, и, соответственно, поможет поднять права локального юзера до r00t`овских. Затронуты версии 8.11 и 8.12 в различных проявлениях (beta 5, 7, 8 и т.д.) Из предыдущих версий безопасными остаются 8.9 и 8.10 (по крайней мере от рассматриваемой дырищи).
Уязвимость притаилась в функции tTflag(), что напрямую завязана с опцией программы -d, т.е. баг становится актуальным при активной d. За полным описанием, как и за готовым эксплойтом, следует лезть в классический багтрек. Сплойт, кстати говоря, написан нашим соотечественником – Александром Юрченко, с названием Алсу -).
http://www.securityfocus.com/bid/3163

Microsoft Outlook Express
by Andrew McQueen <amcqueen@jstmack-intosh.co.uk>
Когда видишь постинги бага в MS-продукте, приходит усталость от скроллинга всех уязвимых платформ: все варианты виндов, с SP, с hotfix`ами и без... Здесь подобный случай. Outlook Web Access – дополнительный модуль Exchange server`а от Microsoft, который в работе тесно связан с IIS-сервантом того же производителя. Дополнительная фича позволяет изучать новые письма по WWW, т.е. преобразует обычную почту в web-ориентированную. Значок % – давнее западло многих систем, из которых не выделился и OE. Система останавливается aka виснет, после того как пользователь вводит нехилую кучу %%% в поле Log On`а. Сие случается как при вводе мусора вместо (вместе) логина, так и пароля. Баг завязан на первичную дыру в WWW Publishing и IIS Administration-сервисах. Дырка разработана не на 100%, так что реальным можно считать выполнение кода в системе жертвы с административных полномочий. Из описания понятно, что для атаки на сервер – эксплойт не нужен, потребуется лишь наличие браузера :). На данный момент официального патча от MS не последовало. Ждем первой звезды.

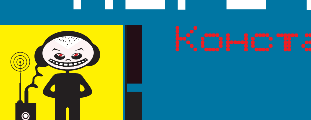
SSI/IIS
by MS Technet

В трехбуквенных сокращениях – потеряться не сложно, тут тебе и IIS, и ISS, и SSI... Сегодняшний случай – пересечение всех трех. 1 – обладатель бага, 2 – средство поиска дыры, 3 – точное местоположение уязвимости. Для интерпретации SSI юзается модуль ssinc.dll. По дефолту ssinc вступает в половую связь с .stm, .shtm и .shtml файлами.
SSI обрабатывает #include:
<!—#include file="Filename"—>
Реагируя с #include, ssinc.dll запрашивает на верность имя папки, где лежит .shtml файл, потом прописывает в конец этот файл и дает новый путь.
Получив имя файла через test.shtml ssinc.dll, чекает объем источника информации (aka file). Когда объем превышает 0x801 байт, ssinc.dll производит обрезание до 0x801 байт и дописывает в конце '\0'. Получается, что имя файла (включая '\0') будет не больше, чем 0x802 (2550) байт. Но на практике ssinc.dll не проверяет длину обновленной строки, где лежит путь, из конца имени текущего каталога. Т.е. легко обустраивается переполнение буфера. Когда (читай – всегда) ssinc.dll обладает системными привилегиями, у атакующего возникает маза выполнить произвольный код с системными правами.
Для эксплойтинга необходимы два условия:
1. Доступ к созданию файла или папки в ВЕБ-директории.
2. Возможность обращения к созданному файлу через web сервис.
Эксплойтим:
1. Создаем файло "xakep.shtml", включающего в тело подобную инфу:
<!—#include file="AAAA[...]AA"—>
Число 'A' следует сделать огромедным, больше чем 2049.
2. Делается папка "a" в каталоге Web. Копируется "xakep.shtml" в "a" каталог.
3. Открываем "xakep.shtml" с помощью браузера:
http: // xakep.ru/a/xakep.shtml
4. IIS вернет пустую страницу. Сие станет известием произошедшего переполнения.

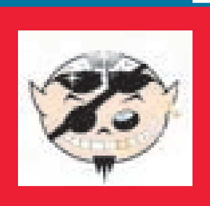
FreeBSD IPFW
by FreeBSD Security Advisory

BSDуны никак не разберутся меж собой: кто лучше – ipf или ipfw. У всех свои доводы. Новый баг станет на сторону ipf-еров. Для эксплойтинга потребуется доступ в систему, т.е. дыра является локальной.
Использование ipfw с "me" идентификатором на "point to point" интерфейсе может повлечь за собой доступ к локальному хосту с удаленного, что находится на другом конце линка. Когда "me" используется на рассматриваемом линке, ipfw создаст специфическое правило в firewall-настройках для удаленного хоста. Созданное правило позволит намеренный доступ в систему, по которому может случиться несанкционированный доступ определенным ресурсам.
Результат достаточно серьезен, т.к. часто в VPN`ах (бывает редкие герои, кто их строит в *nix`ах =) ограничение доступа осуществляется только правилами файрвола, замещая простейшее системное распределение access`а.

Hard news ...



Константин Буряков aka p0r0h (p0r0h@ixbt.com)



Новый прорыв

Свершилось! Вслед за анонсом Creative объявила о начале продаж своей новой линейки звуковых карт Sound Blaster Audigy. Семейство Sound Blaster Audigy состоит из карт Sound Blaster Audigy Platinum eX, Sound Blaster Audigy Platinum, Sound Blaster Audigy X-Gamer и Sound Blaster Audigy MP3+. Звуковухи имеют великолепные характеристики: 24-бит/96 кГц ЦАП (DAC), соотношение сигнал/шум (SNR) - 100 дБ, поддержка Dolby Digital 5.1 и т.д. Сразу рассказать о всех прелестях новинок затруднительно (жди обзора :)), а пока лишь отмечу основные детали. Сам аудио процессор Audigy с фирменными технологиями EAX ADVANCED HD и Multi-Environment позволяет производить одновременный рендеринг до 4 аудио потоков и имеет в 4 раза большую производительность, чем у прошлого креативовского чипсета EMU10K1. В основе фирменных технологий лежат различные интерактивные элементы для удаления раздражающих шипящих и скрипящих звуков при прослушивании музыки, для ускорения или замедления скорости воспроизведения без изменения тональности сигнала и его качества, для широкого диапазона предустановок и аудио эффектов, для создания расширенной картины окружающего звука (enhanced surround sound) с любого стерео источника, а также другие фишки, позволяющие добиться улучшения качества звука как в играх, так и при воспроизведении музыки. Топ-моделью является Sound Blaster Audigy



Platinum eX, имеющий дополнительный Audigy Drive модуль, который соединяется со звуковой платой специальным кабелем и может быть размещен где удобно счастливому обладателю этой звуковухи. Еще одной приятной особенностью всех карт Sound Blaster Audigy является интегрированный интерфейс SB1394 (аналог IEEE 1394 FireWire) для подключения к внешним цифровым устройствам. Sound Blaster Audigy Platinum eX будет продаваться за 250 буказоидов, Sound Blaster Audigy Platinum за 200$, а за модели Sound Blaster Audigy X-Gamer и Sound Blaster Audigy MP3+ просят всего около 100 бакинских. В общем, настало время задуматься о приобретении новой звуковухи ;].

Radeon 2

Недолго GeForce3 единолично царствовал на рынке видеокарт. Канадская компания ATi представила свой Radeon второго поколения. Если первый Радеон не очень успешно конкурировал с семейством GeForce2, то Radeon 2 должен составить очень серьезную конкуренцию топ-модели GeForce3 от Nvidia. Этому способствует отличная архитектура чипа, высокие тактовые частоты и фирменные технологии Truform, SmartShader, SmoothVision, HyperZ II, HydraVision, Charisma Engine II, Pixel Tapestry II, Video Immersion II, значительно улучшающие 3D-графику. Если к моменту появления новых видюх программисты ATI доведут до ума драйверы и все заявленные технологии будут нормально функционировать, то GeForce 3 может оказаться в глубоком анусе. Radeon 2 будет выпускаться в 3-х модификациях. Для хардкорных геймеров предназначен Radeon 8500 с частотами чипа/памяти 250/275 МГц, полная поддержка возможностей DirectX 8.1 и т.д. Плата будет иметь на борту 64 Мбайт DDR памяти, аналоговый, DVI и видео выходы. Первоначальная стоимость составит около 400 буказоидов. Radeon 7500 представляет собой своеобразный Radeon Ultra, поскольку поддерживаются лишь возможности DirectX 7.1, но зато значительно увеличены тактовые частоты чипсета и памяти до 270/230 МГц, а также установлен новый контроллер памяти с отличной пропускной способностью (8.8 Гбайт/с). Объем памяти - те же 64 Мбайт DDR. Ориентировочная цена 200 зеленых у.е. Также компания ATI решила выпустить аналог профессиональной карты Quadro на ядре GeForce. Им будет FireGL 8800, основанный на новом ядре Radeon 2 и имеющий усиленную поддержку OpenGL и Linux. FireGL 8800 будет поставляться в октябре, но с ценой ATI еще не определилась. Судя по всему, новые Радеоны будут весьма заманчивой покупкой. Как бы удержаться до выхода многообещающего чипа Columbia от S3 ;]?



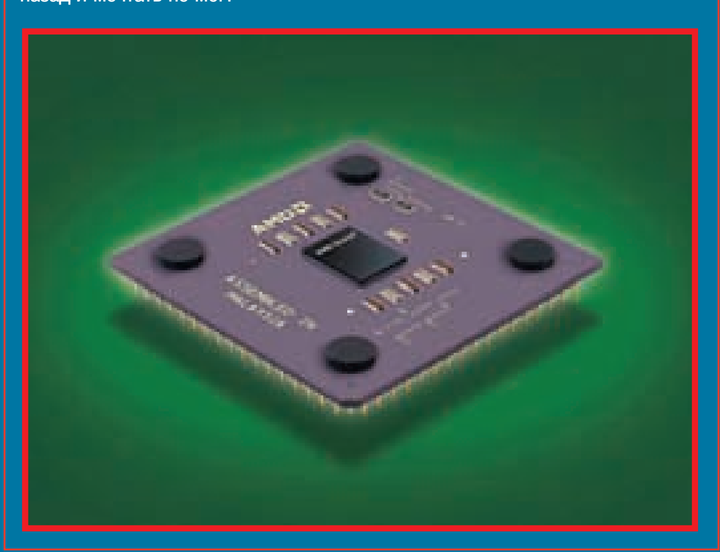
Свободу Клаве!

Именно под таким девизом компания Logitech вполне могла бы продвигать свой новый девайс. Совместив свои последние разработки Cordless Mouseman Optical и Cordless Freedom, Logitech выпустила стильный девайс Cordless Freedom Optical. Основная изюминка - полное отсутствие проводов. Беспроводная оптическая клава делится на четыре базовых управляющих панели, функция каждой клавиши может быть перепрограммирована для запуска прог, различных приложений, открытия сайтов или менюшек (также можно назначить текст подсказки для каждой клавиши). Передняя и центральная панели служат своеобразными мультимедийными центрами, позволяющими дистанционно управлять MP3/CD проигрывателями (например, Winamp или Windows Media Player). Естественно, на клавиатуре существуют клавиши с самыми распространенными командами для копирования, вставки, печати и т.д. О цене точной информации пока нет, но, думаю, сильно завышена она не будет, и юзвери смогут по достоинству оценить интересную новинку.



Гигагерц дешевле 100$

Какая компания? Правильно - AMD ;]. Официально был анонсирован выход процессора Duron на новом ядре Morgan с частотой 1 ГГц. Новое ядро Morgan обладает отличным разгонным потенциалом, высокой производительностью (по сообщениям из забугорных источников он даже обходит Атлоны на старом ядре с аналогичной частотой) и пониженным энергопотреблением, но, пожалуй, самым шоколадным фактом является цена на новенький Дурон - всего 89 баксов. Об этом среднестатистический юзверь года два назад и мечтать не мог.

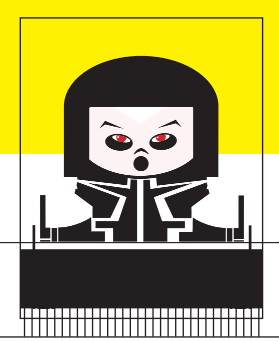


Дешевенький Rio

Компания SONICblue анонсировала выпуск портативного плеера Rio One по цене 99$. Это первый плеер с флэш-памятью с такой ценой. Сам Rio One выполнен на базе известной модели Rio 300 и оборудован USB интерфейсом. Объем памяти невелик - всего 32 Мб, но слот под флэш-карты SmartMedia (до 128 Мб) позволяет несколько увеличить ее. Rio One, помимо поддержки форматов MP3 и WMA, может быть перепрошит под новые версии стандартов (уж лучше бы сразу поддержку MP3 Pro включили :)). В комплект также входит пара батареек АА и наушники средненького качества. Кому нужен компактный плеер (в смысле маленький ;)) и кто готов забить на малый объем памяти, могут смело брать Rio One - один из самых привлекательных девайсов среди флэшовых плееров на сегодняшний день.







MP3/CD плееры

Константин Буряков
aka p0r0h (p0r0h@real.xakep.ru)

выбираем лучший!

Если в метро послушать, пока в универ едешь, - нормал, а если в поезде, который несется в Сочи? В общем, наш выбор - MP3/CD плееры! Сливаешь из Сети любимую музыку, нарезаешь ее на CD-R и слушаешь в течение 30 миллионов лет. А вот на чем слушать - читай ниже.

Аудиокассеты - сакс. CD - более-менее нормально. Минидиски - рулез, но непопулярно. А как там поживает народный MP3-плеер? К сожалению, многие ведущие производители попросту забили на этот стандарт, лишь изредка выпуская сомнительные девайсы - флэшовые плееры. И это тоже полный отстой. Ну что можно запихнуть на 32 (ну пусть 64) мега флэшки?

Lenoxx MP-786

Этому плееру хоть и исполнился почти год, но он остается, пожалуй, самым популярным на нашем рынке, благодаря привлекательной цене и характеристикам. Выглядит же Lenoxx MP-786 как обычный CD-плеер. При выборе плеера следует обратить особое внимание на его размеры и массу. У Lenoxx MP-786 с этим все в порядке - всего лишь 145x130x28 мм при массе 250 грамм (без батареек).

Спецификации

Плеер поддерживает обычные сидюки и MP3/CD на CD-R, CD-RW болванках. Правда, с CD-RW не все так просто - некоторые партии плееров от Lenoxx отказываются их воспроизводить. Но винить тут некого: согласно характеристикам плеер вообще не должен поддерживать перезаписываемые компакты. К размеру же дисков Lenoxx MP-786 относится вполне нормально - никаких проблем с болванками объемом 700 Мбайт замечено не было. Ограничения на общее число файлов и директорий - 512 и 256 соответственно. Думаю, хватит с лихвой ;). Что касается мп3-файлов, то по мануалу поддерживаются лишь битрейты до 224 Кбит/с. На практике же оказалось, что плеер спокойно играл mp3'шки с битрейтом 256 Кбит/с. Существует также поддержка 3-х частот дискретизации: 32, 44 и 48 КГц. Впрочем, мп3'шки с частотами ниже 22 КГц встретить довольно проблематично.

Качество звучания

Наушники, поставляемые в комплекте, - полный слив. Пришлось доставать приличные наушники от Sony. Это сразу же преобразило картину! Причем как при прослушивании классических композиций, так и при рок-, техно- и транс-музыке с различным битрейтом.



Особенности

Навигация по трэкам довольно удобная. Все привычно, как у обычного CD-плеера. А вот с навигацией по директориям дело обстоит немного сложнее. При вложенных директориях придется активно поюзать качающуюся кнопку Play/Stop (при кратковременном нажатии она осуществляет вход во вложенную директорию или выход на один уровень вверх). В эквалайзере присутствует всего пять встроенных пресетов - Normal, Super bass, Bass, Treble, Super treble (для аудиокомпактов только первые два). Дополнительная фишка в виде диктофона является скорее декоративной. Встроенного микрофона в плеере нет, а таскать с собой полноценный внешний только для того, чтобы записать 500 секунд речи, удовольствие не из приятных.
Из приятных фич я нашел антишок на 60 секунд, который отлично справляется со своими прямыми обязанностями, и линейный выход. С его помощью и аудиошнуром, идущим в комплекте, можно проапгрейдить свой музыкальный центр, добавив поддержку CD-MP3.
Да, еще! Блок питания идет в комплекте, поэтому дома аккумуляторы юзать не надо.

Минус: небольшой размер ЖК дисплея - об ID3-тэгах и прочем придется забыть.
Плюс: управление как у обычного CD-плеера, для извращенцев есть функция диктофона.
Цена: 90-100$
Оценка: ★★★★ (Клево!)

NAPA

NAPA сразу же обращает на себя внимание своим необычным дизайном и размером. Да и весит он несколько больше, чем обычные плееры, - 400 граммов. Разработчики NAPA, наверное, планировали свой плеер для использования в качестве недорогого и портативного компонента домашней музыкальной системы, потому как таскать этот кирпич в кармане не кайфово.

Спецификации

ЖК дисплей информативностью не радует. MP3-тэги и даже имена файлов не отображаются. Хорошо, что расположение кнопок управления оказалось довольно удобным. К тому же плеер комплектуется внешним пультом дистанционного управления, поэтому работать с девайсом от NAPA будет достаточно комфортно. Диски NAPA читает легко и непринужденно: Audio CD, MP3 (на CD-R, CD-RW болванках), а также видеодиски (!) в формате VCD. Для MP3-файлов плеер тянет битрейты до 320 Кбит/сек, с частотами дискретизации 22, 32, 44 и 48 КГц.

Качество воспроизведения

С наушниками повторилась та же история, что и с Lenoxx MP-786. Ну нельзя же так портить общее впечатление о плеере! Ну да ладно - пришлось довольствоваться своими наушниками. Никаких обломов при проигрывании обычных музыкальных сидюков не наблюдалось. Впрочем, как и при воспроизведении MP3. Диски успешно читались и довольно добротно играли. Но эта модель меня заинтересовала своей фишкой - VCD. Именно с этим форматом я больше всего провозился, и плеер оставил, пожалуй, самые приятные впечатления. Качество изображения и звука - rulezzz! Смотреть видео на телевизоре было покомфортней, чем на компьютере - пресловутыми “квадратиками” и не пахло. А если вспомнить, что в комплекте идет пульт ДУ, то ты поймешь, почему я так протащился. Именно на управление VideoCD рассчитано подавляющее большинство кнопок на пульте - управление качеством звука, “пошаговый” режим перемотки, режим “дайджеста” диска с картинками, соответствующими каждой дорожке, и т.д.

Особенности

Сразу обрадовала 25-шаговая регулировка громкости звука. Что касается навигации, то NAPA может сканировать папки до 5 уровней в глубину, но вот перемещение по папкам-альбомам невозможно - кнопка “быстрая перемотка” в режиме MP3 позволяла всего лишь делать “скачок” в 10 песен. А если учесть, что ID3-тэги или названия файлов не отображаются, то это крайне неприятный сюрприз. С антишоком тоже не все гладко. При проигрывании AudioCD меня вообще терзали смутные сомнения, существует ли он? Малейшая тряска, и он начинал безбожно запинаться. Зато с MP3 все было в шоколаде - даже если бы я участвовал в Кэмел Трофи, он бы не подвел. Но после всех радостей по поводу антишока я ощутил печаль от сканирования диска MP3. Слишком

долго (10-12 секунд)... Да и паузы между треками (около 3-х секунд) начинают действовать на нервы. Отдельного упоминания заслуживает питание плеера. Батарейки или пальчиковые аккумуляторы плеер не поддерживает, а бесперебойная работа от встроенного комплекта аккумуляторов в режиме MP3 длится всего лишь 45-55 минут (по документации - до 2 часов). Время подзарядки аккумуляторов - 8 часов.
Т.е. час слушаем - восемь заряжаем. Suxxx.

Плюсы: поддержка VideoCD, внешний пульт ДУ.
Минусы: тормоза, нельзя перемещаться по папкам, невозможно посмотреть ID3-теги и названия файлов.
Цена: 110-120$
Оценка: ★★ (Лажа…)

Soul DMP-01

Приятный дизайн напоминает что-то среднее между летающей тарелкой и морской ракушкой. Но не в дизайне дело. Лучше приступим к детальному рассмотрению этого девайса.

Спецификации

Плеер имеет довольно небольшой размер (130x140x30 мм) и вес (235 грамм). К тому же вместе с плеером поставляется неплохой чемодан на пояс, поэтому прогулки с Soul DMP-01 не должны вызвать никаких неудобств. Отличительной чертой Soul от других плееров является большой четырехстрочный дисплей. На нем отображаются ID3-тэги, названия файлов и папок, чего так не хватало юзверям. Вот только необходимость нижней четвертой строки на дисплее вызывает у меня большие сомнения. Дело в том, что на ней изображены какие-то обкуренные пляшущие человечки, которые пытаются танцевать в такт музыке, но это у них не очень-то получается. Лучше бы инженеры Soul разместили вместо них какую-нибудь нужную инфу (например, отображение текущего битрейта). Официальная спецификация Soul DMP-01 говорит о поддержке множества форматов записи и кодеков. Это good. Полная поддержка не только всей битрейтной палитры MP3, но и форматов WMA на болванках CD-R и CD-RW - в общем, все что нужно придирчивому юзеру.

Качество звучания

Наконец-то я увидел в комплекте с плеером наушники вполне хорошего качества! Можно все потестить на родных девайсах. Плеер бодренько заиграл компакты с музыкой в различном формате и качестве. Звучание довольно мягкое и приятное. Эквалайзер со своими обязанностями тоже справляется отлично. Если у Lenoxx'а завышение высоких и низких частот было выполнено с размахом, чтобы сразу добиться явного различия в звуке ("бум-бум" или "умца-умца" :), то аналогичные пресеты Soul явно звучат более сглажено, с не резкой границей. С громкостью у Soul'а тоже все в порядке - 20-шаговая регулировка обеспечит нормальное звучание в любом месте (даже в метро).

Особенности

Кнопки на крышке делали не для удобства, а для красоты. У того же Ленокса кнопки не рассыпаны



по всей поверхности крышки, а сконцентрированы в одном месте. Поэтому его не надо извлекать из сумочки, чтобы проделать какую-либо опера-

цию. У Soul'а кнопки заточены под дизайн. Ну и ладно. Зато у этого девайса есть пульт ДУ. Эта фишка частично оправдала неудобное расположение кнопок. Почему частично? Да, на нем присутствуют стандартные функции: навигационное "колесико", регуляторы громкости, пресеты эквалайзера, переключатель Hold, защищающий от случайного нажатия кнопок, но вот функцию "Navi" разработчики почему-то забыли вынести на пульт. Так что, если захочется перейти с альбома на альбом или на какую-то конкретную композицию, то все равно придется доставать плеер из сумки и уже манипулировать его кнопками.
Антишок мало чем отличается от других плееров. Правда, хоть его буфер и увеличен (120 секунд против стандартных 60), но при пробежке или скоростном кроссе, особенно при проигрывании обычных AudioCD, Soul DMP-01 иногда заикался. Кстати, в процессе тестирования этого плеера открылась одна интересная недокументированная функция. Для доступа к ней необходимо нажать кнопку эквалайзера и удерживать ее, после чего станут доступным: включение и отключение подсветки дисплея, звуковых сигналов и отображения ID3-тэгов. Если отключить эти возможности, то можно несколько продлить заряд аккумуляторов, которые в обычном режиме тянут 10-12 часов. Почему так много? За счет применения специальной технологии проигрывания. Плеер считывает данные в буфер и останавливает диск - до тех пор, пока буфер не будет почти пуст. Таким образом, сильно экономится энергия на пассивной работе двигателя.

Плюсы: огромный дисплей, возможность апгрейда прошивки из Инета, малый расход энергии.
Минусы: кнопки по корпусу раскидывал наркоман.
Цена: 160$
Оценка: ★★★★★ (Рулез!!!)

MiSEL MPJuke-2000

Еще один достаточно продвинутый плеер. Его корпус практически симметричен и имеет небольшие размеры 131x135x34 мм. Да и весит MPJuke-2000 немного - всего 275 грамм. Большой жидкокристаллический дисплей должен радовать юзверей инфой о трэках и о режимах работы плеера.

Спецификации

Начну с главных фич. Во-первых, полная и документированная поддержка CD-R/CD-RW дисков. Во-вторых, поддерживаются ID3-тэги. В-третьих, плеер снабжен удобной системой навигации по директориям EDA (Easy Directory Access). В-четвертых, полностью поддерживаются и отображаются длинные имена файлов и директорий. Теперь понятно, зачем нужен большой жидкокристаллический дисплей ;)? Играет плеер как обычные AudioCD, так и болванки с MP3. MP3'шки могут быть с битрейтом от 8 до 320 Кбит/с (CBR или VBR). А линейный выход позволяет подключить MiSEL MPJuke-2000 к другой аудиоаппаратуре (но шнура в комплекте нет).



Качество звучания

Предобработка звука в MPJuke-2000 осуществляется по-новому: вместо пресетов эквалайзера теперь есть возможности ручной регулировки уровня высоких и низких частот. Вот это - более правильное решение. Только наушники, как всегда, оказались отстоем. Особого смысла в их использовании я не видел, поэтому опять пришлось доставать многострадальные Sony. Благо, что слушать музыку на MiSEL MPJuke-2000 было приятным занятием. Качество проигрывания AudioCD очень хорошее. Даже при подключении аудиосистемы к линейному выходу плеера звук был весьма достойным. Единственное, что не понравилось: громкость при проигрывании AudioCD несколько низковата. Конечно, в большинстве случаев ее хватает, но в сильно зашумленных местах (на дискотеке :) могут возникнуть проблемы. Воспроизведение mp3'шек
тоже радует слух, но не так, как Soul DMP-01.

Особенности

В принципе, в MPJuke-2000 внесена возможность модернизации (заливка новой прошивки) для поддержки новых стандартов сжатия, функции и т.д., но на сайте производителя пока глухо. Навигация по трэкам и папкам очень удобная - благодаря фирменной системе EDA. Производитель существенно облегчил жизнь юзерам и избавил их от необходимости прорываться сквозь хитросплетения файловой системы. Антишока в режиме проигрывания AudioCD вполне хватает, но вот слишком сильных встрясок он немного боится и от страха заикается :). А при воспроизведении MP3 антишоком используется тот же алгоритм, что и в плеере Soul DMP-01: после заполнения буфера мотор останавливается, а когда буфер близок к опустошению, запускается снова. Но даже при этом энергию плеер жрет как первые MP3/CD плееры. К тому же, в комплекте нет зарядного устройства!

Плюсы: супер-информативный дисплей, возможность апгрейда прошивки, ручной эквалайзер.
Минусы: разработчики зажали зарядное устройство и шнур для линейного выхода, на батарейках разоришься!
Цена: 160$
Оценка: ★★★★ (Клево!)

Philips Expanium

Внешне дизайн Philips Expanium выполнен очень удачно: серебристое покрытие, кнопки под металлик, округлые углы, небольшой размер (130/138/32 мм) и вес (250 грамм). Но вот практичность дизайна находится под большим вопросом. Стекло дисплея и фон очень темный. Из-за чего приходится



буквально всматриваться, что за инфа изображена на нем в текущий момент. Расположение кнопок тоже далеко от идеала. Разьем для наушников и регулятор громкости находятся внизу на левом ребре, поэтому, чтобы их постоянно контролировать, плеер приходится постоянно таскать вверх ногами. Зато в комплект входят наушники, блок питания и адаптер для питания от автомобильного прикуривателя.

Спецификации

Плеер распознает обычные сидюки и CD-R/CD-RW с mp3'шками. MP3 играются с битрейтом от 32 до 320 Кбит/с, причем допустимы и "нестандартные" значения. На распознавание дисков уходит в среднем 5-6 секунд, что не так уж и много. А фирменная функция Magic ESP (Magic Electronic Skip Protection) должна защищать диски от сбоев во время проигрывания. Максимально возможное количество треков на диске - 999 штук.

Качество звучания

Вставив обычный музыкальный компакт-диск, я был неприятно удивлен. Звук какой-то плоский, без ярких басов, да и громкость была очень низкой. Смена наушников на более качественные особых перемен не принесла. Режим усиления низких частот (Dynamic Bass Boost) с AudioCD показался вообще бесполезным - этих усиленных басов практически не слышно. Хорошо, что с MP3 дисками плеер вел себя вполне нормально. Звук был достаточно чистый и качественный. Но громкость все равно была ниже, чем у других MP3/CD плееров, а значит в метро не помеломанишь.

Особенности

Управление стандартное, без проблем. Но есть фирменная функция - Resume, позволяющая играть с последнего трека, на воспроизведении которого он до этого был отключен. Причем реализована эта функция в механике, так что, если компакт вынуть из плеера, то "Resume" доступна не будет. Антишок выполнен очень достойно. Особенно при воспроизведении MP3 - сбоев или заикания у Philips Expanium вообще не наблюдалось. Немного хуже дело обстоит с энергопотреблением. Плеер довольно прожорлив - заряда аккумуляторов хватает примерно на 5-6 часов.

Плюсы: отличный антишок, в комплекте идет адаптер для автомобиля.
Минусы: дисплей сосет, энергию жрет с аппетитом, играет очень тихо.
Цена: 170$
Оценка: ★ (Слив)

Апгрейд для хацкера

Павел Тимофеев (netfox@iname.ru)

Почти всегда при апгрейде меняют вместе материнскую плату, процессор и память, ну а если комп совсем старый, то и видяху. А мысль поставить процессор с максимальной частотой, которую держит мамка, и добить побольше памяти в голову юзерам приходит редко. Но настоящий хацкер выжимает из своего компа все возможное и невозможное, при этом обходясь малой кровью (читай малыми средствами). Впрочем, если ты богатый Буратино и отстегнуть 300-400$ на апгрейд для тебя пустяк, то данная статья тебе будет вряд ли интересна. Если же нет, то слухай сюда.

Мама

Пожалуй, одна из самых распространенных конфигураций в России - это комп на базе процессора ip166-233MMX, 32 метра памяти, ну и видяха метра два. Обычно все это работает на материнской плате с чипсетом i430TX (реже на i430VX/i430HX - более древние чипсеты). Официально на платы i430TX максимальный проц, который можно установить, i233MMX. Но в действительности для некоторых плат возможна поддержка процессора фирмы AMD K6-2 3D Now! Небольшая справка по этому процессору: поддерживаемые частоты от 266 до 500 MHz, кэш L1 64 Кб (по 32 Кб для инструкций и данных), кэш L2 (находится на материнской плате) от 512 Кб до 2 Мб. Вот некоторые платы, которые проверенно работают с K6-2: Asus TX97, Asus TXP4, Chaintech 5TDM2, Microstar MS-5158, Shuttle HOT-569 и т.д. Сам понимаешь, все платы перечислить я не могу (да и попросту не знаю), поэтому лезь на сайт производителя, находи описание своей материнки и ищи упоминание о K6-2. Если упоминания нет, то не отчаивайся. Посмотри в документации - поддерживает ли твоя мама питание 2.2 вольта, а также коэффициент умножения 4.5 и, желательно, частоту 75/83. Если да, то тебе повезло :).

Проц

Тут есть некоторые тонкости. Поставить проц 450 MHz можно, но возникновение некоторых глюков не исключено, а может и плата не выдержать (от перегрева). Глюки возникают вот откуда: на платах максимальный множитель 4.5, а частота шины



50/66/75/83, т.е. максимальная частота процессора возможна 4.5*83 = 373,5 мегагерца. Но для PCI устройств стандартной частотой системной шины является 33 (66 MHz/2), и работа на более высоких частотах иногда невозможна. Например, многие экземпляры Voodoo отказываются работать на 83 MHz. Но на некоторых продвинутых платах (Shuttle HOT-569, к примеру) множитель 2 считается за 6. Т.е. 66*6=396 MHz - нормальная рабочая частота для всех устройств. Сечешь мазу? Если у тебя PCI устройства без проблем работают на частоте 75/83, то можно поставить 450 или 500 MHz процессор. Замечу, что процессор K6-2-300MHz встает без проблем почти на любую мамку с чипсетом i430TX. Перед установкой обязательно сбегай на сайт производителя твоей материнской платы и слей последний биос и программку, с помощью которой можно его прошить. Кстати, если не знаешь, то все шаманские операции с перепрошивкой нужно производить под досом. Не забудь сохранить старую копию своего биоса - так, на всякий случай. Если у тебя нет бумажной документации на плату, то слей заодно и ее электронный вариант, который, в основном, представлен в формате pdf (смотреть Acrobat Reader'ом от Adobe).

Оперативка

Как ты, наверное, знаешь, современная SDRAM память имеет несколько стандартов: PC66, PC100, PC133. И предназначена для работы на частоте системной шины, соответственно, 66, 100 и 133 мегагерц. Память, созданная для работы на частоте 133, будет работать и на частоте 66, а вот наоборот, в большинстве случаев, увы, нет. Вышесказанное не относится к чипсету i430VX, т.к. он не понимает большие банки, используемые в новых чипах, т.е. PC100 и PC133 с большой долью вероятности на нем работать не будут или будут, но вместо, например, поставленных одним чипом 64 мег у тебя будет определяться только 32 :(. Память сейчас очень сильно подешевела: новые 64 мб PC133 в Питере стоят всего 19$. А так как известно, что памяти много не бывает, то покупай ее, родимой, побольше.

Видяха

Ни одна современная трехмерная игрушка на 2-4 мегабайтной видяхе нормально работать не будет. К сожалению, на старых мамах нет AGP слота, для которого выпускаются все современные видеокарты. Посему наилучшим решением будет покупка 3D-акселератора, который подключается к видеокарте. Брать что-то ниже уровня Voodoo II 8/12 Мб нет смысла. Стоит он 35/45$ соответственно (речь идет о бэушностях, т.к. такую новую карточку достать уже практически нереально). Карты на Voodoo II обладают т.н. свойством масштабируемости, т.е. чем быстрее у тебя проц, тем быстрее работает видяха. И если процессор работает на 300 MHz и выше, то Voodoo II показывает свою реальную мощь.

Винт

Биос материнских плат с чипсетом i430TX и ниже не понимает винчестеры объемом больше 8.3 гигабайта. И при установке большего по объему винта видно будет только эти самые 8.3 гига. Лечится довольно просто. Наиболее правильный способ - это прошить в маму свежую версию биоса, в которой исправлен этот баг. Для тех, у кого мама не имеет флэшовый биос, можно сделать следующее: скачать с сайта производителя винчестера специальную утилитку, называемую диск менеджером. С помощью нее можно, обходя биос, использовать весь объем винчестера. Но этот метод несет в себе один существенный недостаток. Если ты захочешь, скажем, подрубить свой винт к компу своего соседа (mp3-шки переписать), то ты не увидишь на нем свои данные...

И что в итоге?

Теперь подсчитаем, во сколько обойдется апгрейд. У меня была следующая машинка: мама i430TX Asus TXP4, проц i166MHz (не MMX), память 32 PC66 и видео ATI Rage II 3D 2 мб. Я прикупил K6-2-450MHz за 40$ (свой проц продал за 25$), купил память 64 мб PC133 за 19$ и Voodoo II 12 мег за 45$. Разумеется, проц и Voodoo бэушные. Итого за 79$ я получил более-менее нормальную тачку: K6-2-450/96/2+Voodoo2-12, на которой легко бегают Quake III и UT. А если ты в игры не играешь (и правильно), то оставшиеся деньги лучше потратить на покупку оперативки или большого винта.

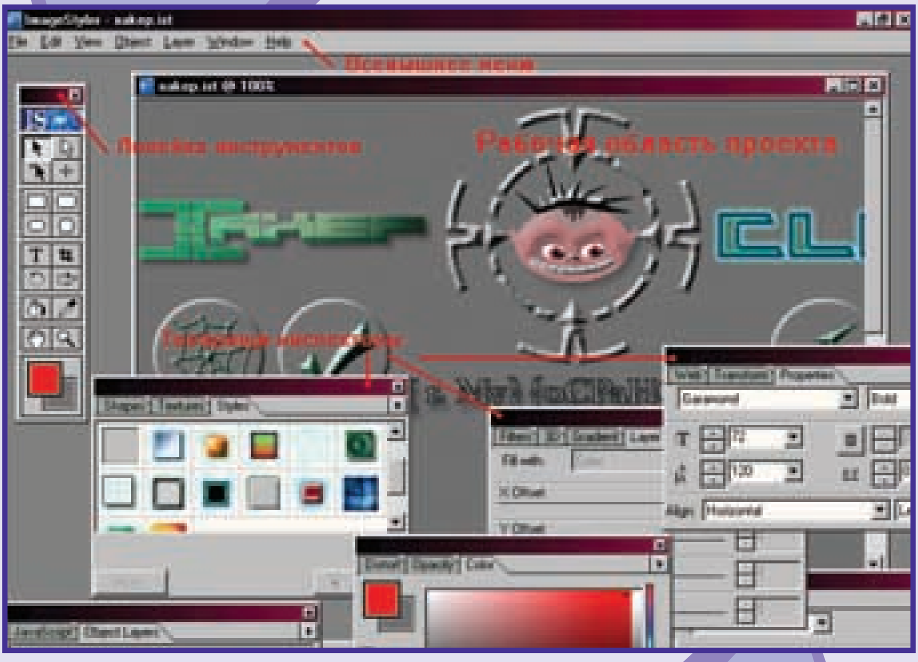


ВыWEBнись Stylьно! тестируем ImageStyler

Donor (donor@real.xakep.ru)

Мазафака! Сколько можно натыкаться на убогие паги и текстовые дефейсы? Маза хакаеры! Пага - это же ваше лицо! А, ну да, конечно, тут у нас 31337-ые хАксОры затесались, которые считают, что text mode - это элита, а любой GUI - для лохов.

Ребятки, идите читать Е-Зины фанатов Роботрона. А всем нормальным чувакам посвящается эта статья. Не надо быть мега-дизигнером, чтобы создавать хорошие паги. Ты же не собираешься побеждать на никарагуанских конкурсах "Пага года"? Ты же нормальный чел, который хочет на свой паге дать людям какую-то важную инфу и поделиться своими мыслями. Я тебя порадую: небольшая заокеанская контора "ADOBE" в беспрестанной заботе о нашем благополучии и наполнении своих банковских счетов сварганила рулезную прогу по кличке ImageStyler. Сейчас мы с тобой заценим все ее фичи и заюзаем их на полную мощность.



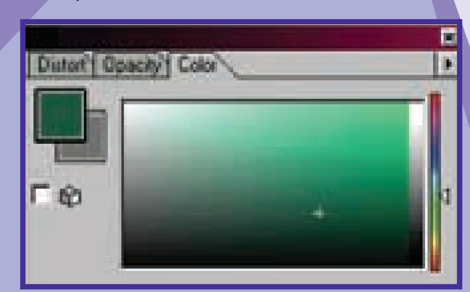
Инспекторы навалились на проект. Надо распихать их по углам.

Чего дают?

ImageStyler - это тулза для быстрого создания вебграфики. Ты можешь загнать в него любые изображения или рисунки и грязно надругаться над ними, применив различные стили, эффекты и трансформации. Также эта софтина поможет тебе красиво раскидать замученные картинки по паге, наделать кнопарей, реагирующих на грызуна, абсолютно не трахаясь со скриптами, сварганить html'ку, порезать и импортировать графику в gif или jpeg. Очень вкусно то, что прога поддерживает слои в объектах, то есть можно творить действительно сложные картинки.

Чего не дают?

К сожалению, не дают разметить html-таблицу самостоятельно. ImageStyler делает это автоматом, причем далеко не всегда лучшим образом. Из ImageStyler'а нельзя загнать в пагу текст. Это все потому, что жадина "ADOBE" позиционирует свою софтину как графическую, а для создания сайтов предлагает купить еще одну (GoLive). Но мы обойдемся. У тебя же блокнот в руки интегрирован ;).

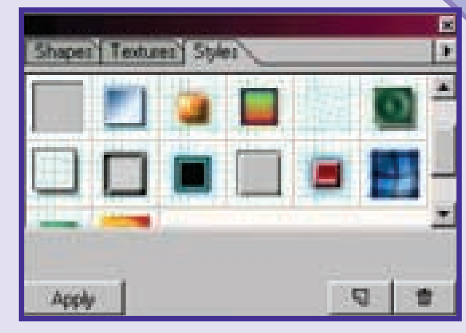


Выбор оттенка морды лица объекта

Как это выглядит?

Разве название производителя не говорит само за себя? Да, выглядит это почти как Photoshop (собственно, на его движке и делался ImageStyler). В открывшемся окне перед тобой картинно разложат проект, линейку инструментов и несколько инспекторов. Инспектор - это маленькая форточка с закладками, через которую ты можешь быстро осуществить какое-нибудь издевательство над объектом (применить стиль, масштабировать, повернуть, изменить цвет и т.д.). Остальные важные функции засунуты в верхнее меню.

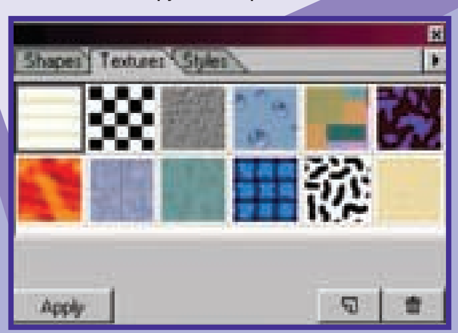
Внешне ImageStyler отличается от Photoshop-а тем, что нет инструментов для рисования и редактирования исходного изображения: работать можно только с готовым объектом. Но, поверь, больше тебе ничего и не понадобится.



Стильная форточка

Давай забацаем чего-нибудь!

ОК! Сделай, например, сайт "][-клуб" и собери на нем вместе всех рульных парней и девчонок своего



Склад текстур. Срочно натянуть!

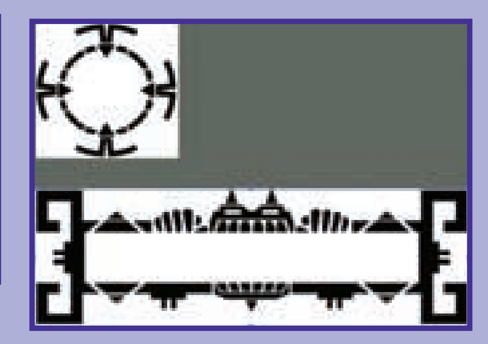
Например, можно взглянуть на текстуру через линзу.

города. Устанавливай и запускай программу. Перед тобой сияет девственной белизной окно проекта и мешаются инспекторы. Распихай их по краям - сейчас мы будем творить. Найди инспектор с закладкой "Color". Это палитра. Выбирай цвет по вкусу. Теперь нажимай на тулзу "Paint Bucket" (помойное ведро) на линейке инструментов и заливай поле цветом. Молодца! Теперь хватай инструмент "Текст" (буква "Т") и тыкай им в поле (о русификации проги читай врезку). Настраивай шрифт в вывалившемся окне,

Вот такие жестокие издевательства претерпело наше лого.

загоняй текст и жми "OK!" Что, нету текста, одна рамка? Да просто он у тебя того же цвета, что и фон! Лезь в палитру и выбирай другой цвет.

А вот теперь - час потехи!!! Посмотрим на возможности ImageStyler-а. Найди инспектор с закладкой "Styles". Выбирай любую пиктограмму и

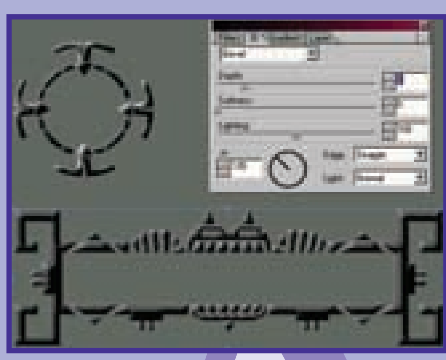


Вот такие рамочки я намутил в Photoshop. Нижней можно стильно оформить баннер.

дави "Apply". Теперь твою надпись не узнать. Если не нравится, нажми Ctrl+Z.

Теперь дави закладку "Textures", выбирай, что нравится, и жми "Apply". Кстати, можешь добавить свою текстуру (квадратик с загнутым углом). Это еще не все! Найди форточку с закладкой "3D" и выпадающий список с надписью "None". Щелкни по треугольничку и поиграй с разными псевдо-3D эффектами. Ниже можно настроить параметры эффекта (яркость, размытие). И это еще не все! Натяни на надпись текстуру. Теперь найди закладку "Distort" и выбери что-то из списка и поиграй с настройками.

Ну как, почувствовал себя извращенцем :)? Комбинируя эффекты, ты всегда можешь забацать



Ну! Совсем другой вид!

что-то необычное.

Но одним текстом сыт не будешь! Не вопрос! Найди закладку "Shapes". Тут валяется набор готовых форм (стрелочек, звездочек, галочек и прочей лабуды). Выбирай любую и дави "Place". Когда форма появится на поле, с ней можно будет сделать все, что ты только что делал с текстом. Но самое замечательное то, что можно импортировать свои формы.

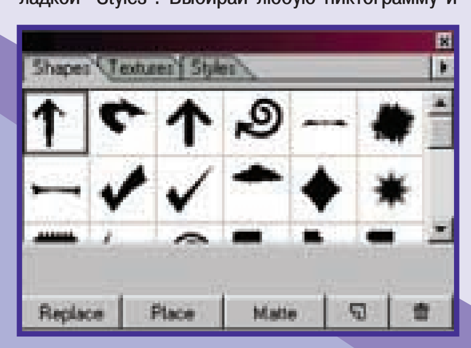
Плагины

ImageStyler поддерживает plug-ins (плагины). Но, к сожалению, все имеющиеся модули связаны с импортом и экспортом в различных векторных и растровых форматах или работой со сканером. Плагинов, добавляющих проге стилей или фильтров, я не встретил, несмотря на самые тщательные поиски. А сам ADOBE перестал поддерживать ImageStyler - ну не пошел он на рынке.

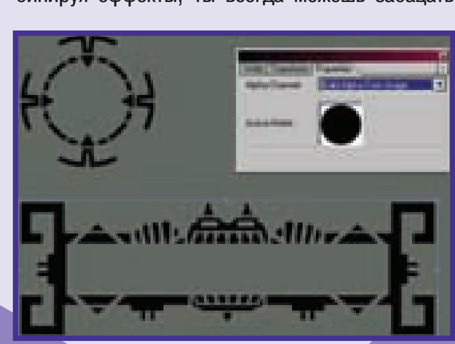
Нарисуй в Photoshop-е какую-нибудь фигуру, например, женскую, закрась ее одним цветом и сохрани ее в jpeg-е (он весит меньше). Теперь лезь в ImageStyler. В меню "File" выбирай "Place..." и находи свой файл. Дави "Открыть". Рисунок появится в поле, но на белом фоне, и ничего с ним пока сделать нельзя.

Найди закладку "Properties" - там ты увидишь выпадающий список. Выбирай пункт "Build alpha from image" (построить альфа-канал или канал прозрачности, из изображения).

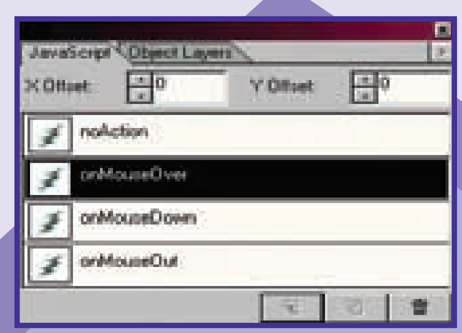
Твоя женская фигура станет полупрозрачной, зато избавится от фона, и ты сможешь сделать ее стильной и красивой. Если ты нарисуешь фигуру в Иллюстраторе, то ImageStyler без проблем откроет ai-файл. С такой формой можно работать сразу: фона там не будет.



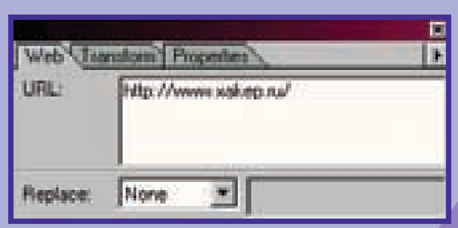
Звездочки и точки, стрелки и крючочки.



Отрезали лишнее.



Инспектор мышиных поз.

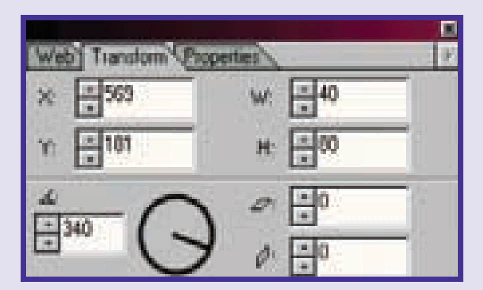


Послать всех по адресу из трех букв!

Эй, а как же кнопочки?

Легко и непринужденно! Нарисуй какой-нибудь кружок или квадратик и пока с ним ничего не делай. Вытащи на свет божий окошко с закладкой "JavaScript"... Не вибрируй! Кодить не надо ничего! В форточке виднеются какие-то слои а-ля Фотошоп. Таким макаром в ImageStyler-е оформлены мышиные позы при контакте с батоном: мышь где-то бродит (noAction), мышь сверху (onMouseOver), мышь притиснула кнопарь (onMouseDown), мышь слезла с кнопки (onMouseOut). Первый слой белый, и рядом мордочка твоей кнопки, остальные - серые. Это значит, что объект пока еще не кнопка, и Яву на него вешать не будут.

Внизу инспектора виднеются листочек, двойной листочек и помойка. Дави один листочек. Второй слой ожил. Все, поздравляю - у тебя родился button. Но просто родить мало! Надо бы сделать,



Циферки, циферки! Все в циферках!

чтобы что-то менялось от тесных объятий с крысенышем. Кликни на второй слой. Теперь можно поменять цвет кнопки, применить 3D-эффект, стиль или текстуру натянуть. Вот так кнопка будет выглядеть при наведении курсора.



Следующий слой лично я делаю, как и второй (из экономии времени и дискового пространства). Для этого шлепни двойной листок, и слой скопируется. А вот последний слой должен быть таким же, как и первый, иначе после ухода мыша в другие края кнопка не вернется в прежнее состояние. Вывод: снова давим одинарный листок. Если какой-то слой не получился или просто надоел, юзай помойку.

Цапа пашет, но не так, как нам надо. В чем дело? А в том, что по умолчанию скромные ребята из ADOBE пошлют нас прямиком на www.adobe.com, что тебе, ясен пень, не нужно.

Нужно, чтобы кнопка отправляла Осла по адресу вроде этого: www.xclub.coolfreehost.ru/images/tetka1.htm или www.xakep.ru. Пофикси эту багу при помощи закладочки "Web". В поле, подписанное URL, воткни свою рульную урлу. Теперь все в порядке.

Пора!

Теперь пора замутить свою пагу. Выбери размеры страницы (лучше всего 800x600) и выстави их в ImageStyler-е, используя пункт меню "Edit/Canvas Size". Помести и разложи на рабочем поле формы и текст, который будет графикой. Применяй эффекты и стили, делай кнопки.

Ты можешь столкнуться с такой проблемой: нужно положить один объект на другой (рельефный значок на рельефное основание, например), а нижняя тварь упорно лезет на верхнюю и скрывает ее от глаз людских. Дело в том, что нижний объект попал на поле позже, а следовательно, и лежит "выше". Изменить эту неприятность можно через меню: Object/Arrange/действие. Действия такие: вытянуть наверх (bring to front), приподнять (bring forward), приспустить (bring backward), загнать на дно (bring to back).

Чтобы удобнее было расставлять объекты по будущей паге, подгонять их по размерам и вращать в разные стороны, пользуйся прокладочкой... в смысле закладочкой "Transform". Тут все в цифре, так что тюнниг проекта пройдет легко.

Учим ImageStyler ругаться по-русски

Styler выцепляет шрифты из папки Fonts твоих Окошек, но далеко не все шрифты будут им опознаны. Поэтому ты можешь не найти ничего русскоговорящего в настройках текста. Дело в том, что этому привереде нужны шрифты в кодировке KOI-8, и желательно, чтобы в поле Version был указан производитель. В W'2000 такой траблы нет.
Если нужные шрифты так и не нашлись, придется импортировать готовые слова в виде форм из Фотошопа :(.

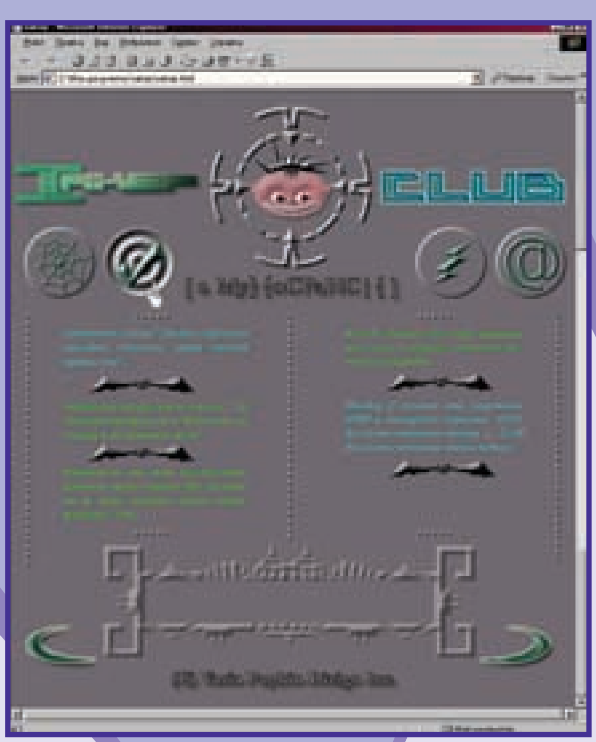
Увидеть!

Да, хотелось бы увидеть, как это все будет функциклировать. OK! В ImageStyler-е есть предпросмотр. Пункт "File/Preview In" позволяет глянуть на дело рук своих в Осле и Фотопопе. При просмотре в браузере задействуются кнопочки, и ты сможешь по ним пощелкать. Также проявятся баги в расположении картинок на странице (что-то съехало, кто-то торчит не по центру и т.д.), и их можно будет сразу прибить.

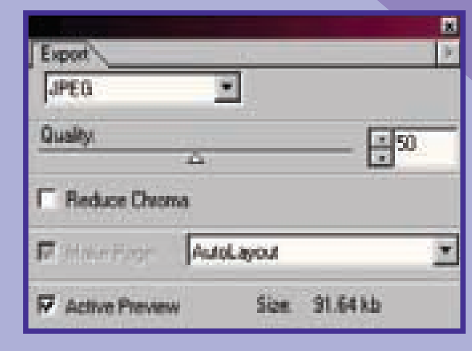
Льготы экспортерам

Теперь надо получить собственно то, что ты вывалишь в iNet. Для этого проект нужно экспортировать. Вытягивай за уши инспектора с надписью "Export". Вот это очень удобная фича. Тут собраны все настройки экспорта плюс еще сразу оценивается вес будущей страницы при таких параметрах. Что такое формат экспорта, понятно. Это jpeg, gif, photoshop. Качество тоже трудностей вызвать не должно. Задействуй check-box "Active Preview" и сразу увидишь, как вес паги зависит от качества графики. Кстати, изменение этого качества ты тут же заметишь прямо в рабочей области. Дальше нужно выбрать способ экспорта (выпадающий список рядом с надписью "Make page"). Первые два способа делают бооольшой скрин твоей паги для самостоятельного нарезания. Третий импортирует объекты в отдельные файлы, но страницу не делает (если ты загрузишь html-ку, все картинки будут положены в столбик, одна под другой). Четвертый (AutoLayout) - автоматически монстрячит страницу. Выбирай его.

Пусть тебя сильно не пугает цифирь в 60-100 кило, если в твоем проекте много одинаковых объектов (кнопочки, бордюрчики и т.д.). Это вполне фиксибельно. В общем, дави "File/Export", выбирай папку, вводи имя файла и жми "Сохранить". В выбранной дире появится html-ка с тем самым имечком и папка Images с jpeg-гами.



Вот такая страница получилась у меня после 40 минут творчества.



Таможенник... в смысле, инспектор экспорта.

Оптимизация посредством кастрации

Если ты расположил свои объекты не одной большой кучей, а оставил между ними небольшие промежуточки, то прога порежет их вполне нормально, то есть один объект - один jpeg. Но если картинки и надписи слиплись вместе, то ты получишь самые немыслимые куски своих творений. Поэтому располагай все посвободнее.

С оптимизацией у этой софтины очень туго. Допустим, ты разграничил колонки текста столбиком рельефных точек. Каждая точка для ImageStyler-а - отдельный файл. И ему плевать, что они идентичны. Скажешь, что вес такой точки - мизер. Да, 400 байт, но у меня их набралось 120 штук, или 46 килобайт(!), и еще 119 лишних файлов. Половина веса паги - мусор! А еще есть кнопочки, каждое состояние которых (при контакте с мышкой) тоже отдельный файл, то есть 4 вместо 2-х (помнишь, не нажатое и отпущенное состояния и наведенное и нажатое состояния обычно совпадают). Что же делать?

Есть два способа: цивилизованный и дикий. Цивилизованный заключается в импорте изображений в Фотошоп для доводки и подрезания либо сразу в jpeg и в использовании визуального html-редактора (GoLiv-

В поисках утраченного

На момент написания статьи ImageStyler (try-ная версия) еще был доступен для скачивания с адобовских сайтов. Но есть все основания полагать, что к моменту выхода номера в свет эту возможность киланут. Я слазил на www.filesearch.ru и в расширенном поиске задал следующие параметры: название файла - is1try.exe и размер файла не менее 100000 байт. По крайней мере три рабочие ссылки я наковырял. Устранить некоторые неприятные ограничения и избавиться от разных противных напоминаний поможет всемирно любимая… 8).

а того же самого). Дикий означает, что ты создаешь страницу ImageStyler-ом со всеми недостатками, а потом кастрируешь их Блокнотом. Сейчас объясню как.

Грузани страницу в бродилке. Теперь кликни на изображение своей точки правой заклепкой мыша. Ты получишь инфу о файле: его название (что-то вроде projectimage7.jpg) и размеры изображения. Сделай backup-копию проекта. Теперь открывай html-ку в Блокноте и ищи в тегах таблицы (<td> и <tr>) название первого файла, содержащего точку, запоминай значения параметров width и high. Далее все imageX с такими параметрами заменяй названием самого первого файла. Удаляй лишние файлы из директории Images. Грузи страницу в Осле и мучительно вспоминай, что же такое не то ты удалил 8).
Также можно вносить и текст. Загнать в макет страницы прямоугольники, на месте которых должны быть слова, а потом, правя файло в Блокноте, заменить их на эти самые слова.

Казнить нельзя помиловать!

Вот, запятую в предыдущей фразе тебе придется ставить самому. С одной стороны ImageStyler позволяет просто элементарно забацать красивые надписи, эмблемки, бордюрчики и прочую графическую мишуру для твоего сайта, причем богатство настроек дает возможность добиться чего-то неповторимого. Кроме того, тебе не нужно будет резать уже готовый проект на части - это будет сделано за тебя. Но, с другой стороны, чтобы комфортно работать с этой софтиной, тебе понадобится еще туча других: Фотошоп, Иллюстратор, GoLive - в общем, почти вся линейка ADOBE. Вот такой неслабый PR :). Если все это у тебя и так есть, имей, однозначно! Если чего-то не хватает, то готовься качать проги и насиловать Асталависту. Ведь приличный угол в iNet-е иметь все-таки хотца!

Своя страничка в Инете от и до
Руководство чайника

Андрей Каролик (andrusha@sl.ru; www.dal.net.ru)

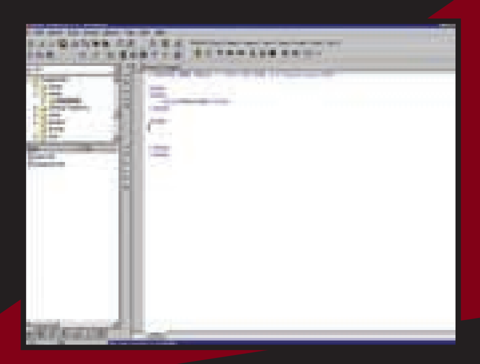
Интернет - это не только информационный фонтан, но и масса возможностей реализовать себя. Одна из которых - состряпать свою собственную страничку. Что именно там будет: ты на горшке, тузик на диване или любимая игрушка детства - дело сугубо личное. Я же поведаю, как использовать html-редакторы и какие из них предпочесть. Ну и, конечно же, расскажу, как и куда потом все это деть.

Что такое HTML?

HTML в переводе с пингвинского означает язык разметки гипертекста (HyperText Markup Language). Сразу развею миф, что html - язык программирования. Нет, это именно язык разметки, а не программирования. Html-документ представляет собой обычный текстовой ASCII-файл с командами форматирования - тегами (tags), содержащими информацию о компоновке документа: стиля текста, заголовках, абзацах, списках, гиперссылках и т.д. Можно, конечно, набирать теги и вручную, что и делают многие бывалые в html-е, но начинающим стоит начать с html-редакторов. Существует множество программ, предназначенных для создания html-документа или преобразования уже готовых документов в html-формат, в народе они обзываются html-редакторами. Html-редакторы избавят тебя от необходимости вручную вводить теги. Некоторые редакторы также позволяют делать проверку синтаксиса html. Типа проверки орфографии и синтаксиса в Word-е, только проверяется правильность написания и открытия/закрытия тегов. Но об этом ниже. Сам html-документ имеет расширение *.html или *.htm. Разницы никакой, просто первое пошло от юниксовых тачек, а второе от виндовых.

Какой HTML редактор?

На сегодняшний день существует много html-редакторов, и начинающим юзверям на первое время подойдет любой. Я рекомендую Macromedia Dreamweaver 2 или Allaire HomeSite 4.0. Обе программы прекрасно сделаны и обладают практически одинаковыми возможностями. Но Dreamweaver ориентирован на более профессиональную категорию пользователей и более навороченен по сравнению с HomeSite. В его библиотеке полно всяческих шаблонов, апплетов, примеров, схем и готовых решений. На первое время тебе это просто не нужно. А навороченность только выйдет боком. Поэтому начни с HomeSite, а проблем с дальнейшим переходом на Dreamweaver у тебя не возникнет, так как у Dreamweaver полная совместимость с HomeSite, Flash, Fireworks и т.д.



HomeSite 4.0

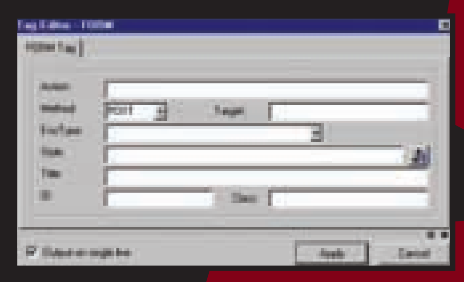
Один из лучших html-редакторов на сегодняшний день. Позволяет вводить любые теги html нажатием на кнопочки аналогично визуальным дельфям. Просто тыкаешь на кнопку любого тега, допустим, формы. В результате получаешь диалоговое окно, в котором вводишь все параметры для тега формы, а после нажатия Apply программа сама генерит соответствующий код. Ты даешь ценные указания программе - программа работает на тебя.

Кроме обычных тегов программа умеет генерить html-код для скриптов, ява-скриптов и апплетов. Очень удобно для начинающих, т.к. эта фича дает тебе вполне рабочий результат, но избавляет от напрягов с кодингом. В первый раз сложно запомнить, как именно пишутся теги, какие параметры находятся внутри каждого отдельно взятого тега, какие являются закрывающимися, а какие нет и т.д. Html-редактор поможет с этим справиться.

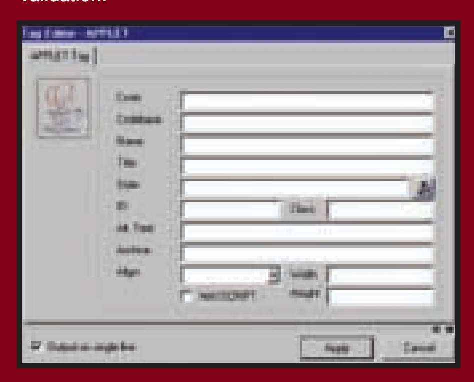
Но то, что программа сама все за тебя генерит, вовсе не означает, что ты не можешь вмешиваться в процесс написания кода. В любой момент в окне Edit (текстовой режим редактирования) ты можешь править код вручную, а результат смотреть в окне Browse. После того как сгенеришь какую-нибудь фишку, обязательно загляни в исходник и посмотри, что там получилось в виде кода. Попробуй что-нибудь изменить и опять посмотри, что получится. Не бойся экспериментировать. Только постоянно практикуясь, ты сможешь что-нибудь реально понять. Если тебе нравится копаться в исходнике, то для тебя окно Design. Оно позволяет делать изменения визуально (визуальный режим редактирования). То есть аналогично Browse, но с возможностью править. Очень удобно. Сначала ты набиваешь пагу в текстовом режиме редактирования, периодически просматривая в окне Browse, как она будет выглядеть в браузере. А в конце подметаешь внешний вид в визуальном режиме редактирования.

Ни нада дилать ашипки

Очень ценной функцией является проверка орфографии и правильности написания и закрытия тегов. Орфография, правда, проверяется только на английском, но тоже иногда не помешает. А вот проверка правильности написания и закрытия тегов на первое время будет твоей козырной

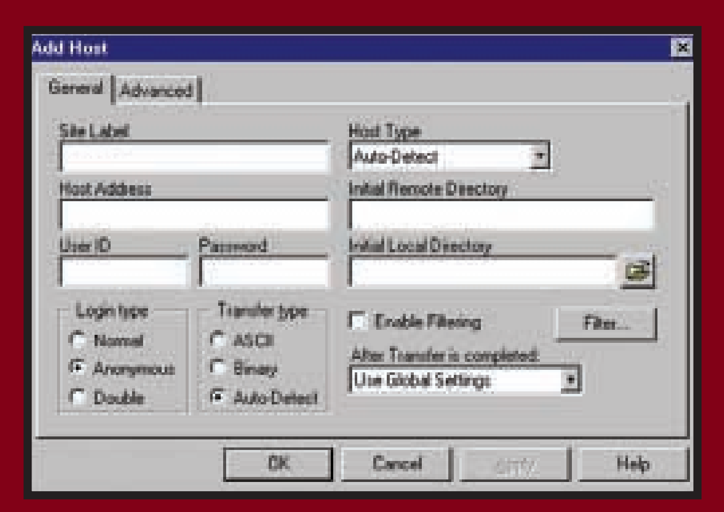


фичей, особенно если будешь править код вручную. Когда код состоит из 5 предложений, ошибки - не проблема. Но когда он состоит из нескольких листингов - становится напряжно. Даже самый простенький незакрытый тег можно искать несколько минут. Программа же найдет его за считанные секунды. Топай в Tools -> Validate Document. Результат проверки появляется в виде отчета на нижней вкладке Validation.



Еще можно выделить возможность глобальной замены и глобальной правки по всем документам проекта. То есть твоя пага будет представлять собой один проект, а внешне отображаться древовидной структурой в том случае, если она состоит из нескольких хтмл-ек. И если в каждом файле есть одинаковый кусок, например, меню, то не нужно будет при изменении меню править каждый файл. Просто топай в Search -> Extended Replace. Там вводи требуемый кусок, на что его

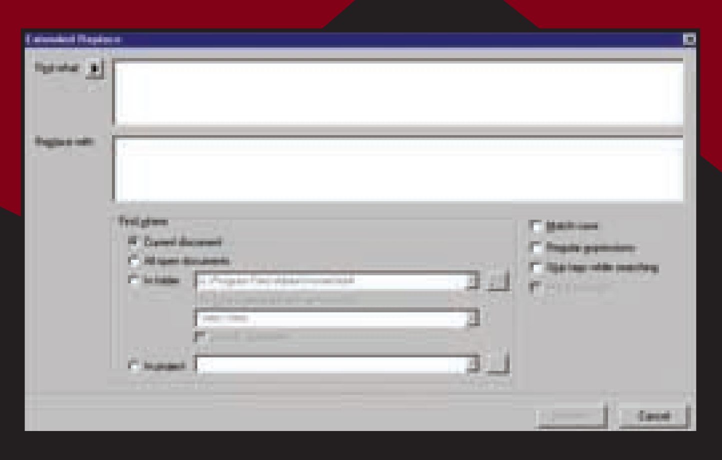
заменить и в каких файлах/папках/проектах его заменять.
Когда ты, наконец, закончишь “кодить”, сохрани всю эту радость привычной комбинацией File -> Save as. Файл титульной (заглавной) странички надо назвать index, тогда по умолчанию он будет грузиться первым. Расширение



либо *.htm, либо *.html - не принципиально. Осталось только выложить свое богатство в iNet. Для этого тебе понадобится место, куда выложить, и фтп клиент (FTP Client).

Куда выложить?

Тут существуют три пути решения проблемы. Либо используй место, которое выделяет твой провайдер, обычно это не более 2-3 Мб дискового пространства на его сервере. Либо купи себе хостинг, тогда объем выложенной информации будет пропорционально увеличивать сумму за хостинг. Хотя обычно предлагается фиксированный объем дискового пространства независимо от того, весь ты его займешь или только часть. Третий вариант - используй бесплатный хостинг. Чаще всего прибегают к первому. Почему? Хостинг твоего прова тебе доступен по определению - это бесплатная услуга. Так почему бы ею не воспользоваться? В отличие от бесплатного хостинга, тут ты всегда сможешь требовать работоспособности своей странички и быть уверенным, что она упадет только тогда, когда упадет весь сервак провайдера. Тебе дадут адрес хостинга, логин и пароль. Можешь воспользоваться и бесплатными хостингами, но их плюсы и минусы я оценить не могу, места в X мало :). Осталось только закачать.



Как закачать?

Чтобы что-то куда-то закачать, нормальные чуваки используют ftp-клиенты. Аналогично html-редакторам их существует бесчисленное множество. Я советую использовать CuteFTP 3.5 и выше. Софтина очень простая и обладает всеми необходимыми функциями. Более профессиональный вариант - SecureCRT. Эта прога вроде бы шароварная, но ты ведь помнишь об astalavista.box.sk? Кроме того, работать она будет даже в шароварном варианте, просто постоянно будет показывать надоедливый баннер, а при истечении 30 дней начнет предлагать зарегистрироваться.
Сразу после запуска открывается Site Manager. Тыкай в Add Site, получишь следующее:
Хоть глаза и разбегаются, по существу тебе потребуется заполнить только четыре поля:
Site Label - просто название для себя, чтобы отличать потом от других.
Host Address - адрес хостинга.
User ID - логин.
Password - пароль.

Теперь жми OK, и дело в шляпе. Ты создал ярлычок для коннекта. Дважды на нем ткни, и коннект пойдет. В результате ты попадешь на свой хостинг. Ты при этом, естественно, должен быть в Инете :). Отображение подобно проводнику в стеклянных, только слева - это панель твоего винта, а справа - сам хостинг. Можешь заливать, можешь сливать. Делается либо двойным кликом на переносимый файл, либо перетягиванием с одной половины на другую. Удачи в переливании и веб-мастерстве :).

Джентльменский набор

эти проги должен иметь каждый

Антон Карпов (toxa@real.xakep.ru)

Доброздравия, приятель. Когда говорят "хацкерский софт", то понимают под этим все что угодно, тем или иным образом относящееся к взлому: начиная от банальных нюкеров, портсканеров и переборщиков паролей и кончая дизассемблерами с шестнадцатеричными редакторами. Но давай разберемся, что действительно надо такому чуваку, как мы с тобой: давно уже переставшему забавляться с нюкерами и прочей подобной ерундой, но еще не доросшему до того уровня, когда весь софт, тебя окружающий, написан исключительно под *nix и исключительно тобой самим, и ты, признанный гуру хака, из *nix'ов не вылезаешь, ибо никсы есть рулез :).

Короче говоря, сейчас я поведу речь о тех программах под Win32, без которых трудно представить жизнь нормального хацкера (каково звучит - "нормальный хацкер"? ;-). Разумеется, я не претендую на объективность и всеобъемлемость обзора, ибо всяческих софтин для перебора паролей, извлечения ресурсов, сканирования удаленных машин и прочая-прочая написано так много, что для описания их всех не хватило бы даже такого объемного носителя информации, как тот, который ты сейчас держишь в руках. А посему ниже я представлю только те проги, которые уже долгое время живут конкретно у меня на моем винче и которые я активно юзаю в разные периоды своей бурной жизни. Если некоторые из них тебе приглянутся и статья подвигнет тебя на то, чтобы слить себе экземплярчик, - что ж, я буду только рад.

Что нам нужно в этой жизни?

Для начала давай определимся, что именно должно входить в понятие "джентльменский набор". Если первое, что тебе приходит на ум, это софтина под названием "нюкер", весь интерфейс которой: одно окошко - для ввода IP, и одна кнопка - "убить гада", то ты сильно не прав. Времена нюкеров прошли, и теперь замечательный листинг под названием winnuke.c можно разве что распечатать (в знак уважения) и обклеить распечатками стены ватерклозета. Я не думаю, что в Сети осталось большое количество юзеров, сидящих под дырявой версией виндов (хех, давненько я не видел в работе такое чудо, как Win95), причем без какого-либо файрвола или хотя бы банального Nuke Nabber'а. А посему позволь мне утверждать, что необходимый хацкеру минимум это:

- утилита для подбора пароля к мылбоксам и другим сетевым сервисам;
- сканер расшаренных ресурсов в локальной сети или Инете;
- редактор ресурсов для вскрытия и потрошения экзешников и dll-ок;
- утилита для выдирания паролей из соответствующих файлов :);
- сканер портов удаленной машины (группы машин);
- какая-нибудь универсальная прога для получения полезной инфы об удаленных серваках;
- дизассемблер и HEX-редактор для копания в кишочках у шаровары.

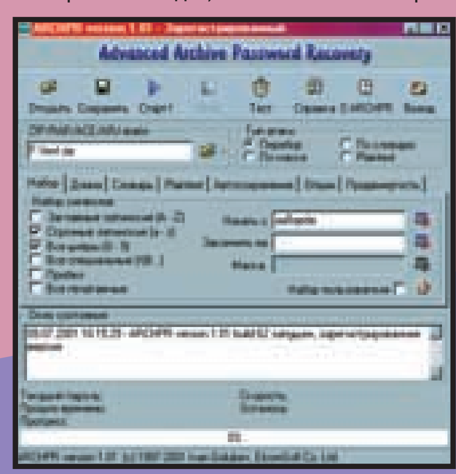
Как я уже говорил, всевозможных прог - тьма, поэтому смотри, чем пользуюсь я. Если ты предпочитаешь другие утилиты - твое дело, о вкусах, как известно, не спорят: я знавал одного чела, так он обожал поедать сливочное мороженое с сушеной редиской вприкуску и утверждал, что это мы все лохи, так как не понимаем смысла истинного вкуса.

Номер ноль: ломаем архивы

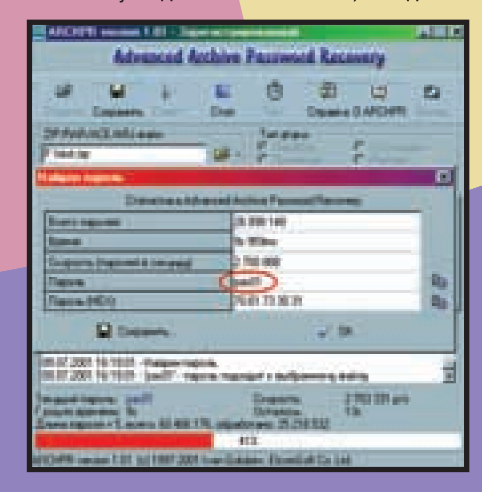
Ты никогда не попадал в ситуацию, когда в каком-нибудь zip или rar архиве валялся ну очень нужный тебе документ, а архив был запаролен, чтобы такие, как ты, туда почем зря не лазили? Вот поэтому мы будем юзать Advanced Archive Password Recovery, или, проще, ARCHPR. Актуальная версия (на момент написания сего труда) - 1.01.

Глупо спрашивать, что может делать эта софтина: на скриншоте видно, что количество настроек очень прилично: можно подбирать пароль как брутфорсом, так и по словарю. В первом случае можно выбирать, какие символы использовать при переборе (только буквы, буквы и цифры, с учетом регистра, без учета оного, включая спецсимволы или без них...), задавать приоритет использования прогой ресурсов машины. Также полезна опция задания максимальной и минимальной длины подбираемого пароля: если ты ломаешь собственный zip-файл по причине того, что пароль вылетел из твоей ветреной головы, но, тем не менее, ты твердо помнишь, что пасс был шестисимвольный, и никаких цифр ты не использовал, то какой смысл выставлять настройки по максимуму, увеличивая тем самым время перебора в разы. Для удобства в объемной работе прога автоматически делает сохранение текущего сеанса каждые N минут, где время между автосохранениями ты выставляешь сам, как пожелаешь. Так что пароли от арха с эксклюзивными фотографиями Лолы Лолобриджиды будут-таки доступны тебе всего лишь через до фига часов, до хрена минут, а никак не позже. Потому как даже если комп зависнет, ты будешь продолжать ломать арх с момента последнего автосохранения.

Ко всему вышеописанному добавлю, что эту прогу с отличными возможностями и удобным интерфейсом написал наш, русский чел, что окончательно убеждает нас всех в том, что данная



Количество настроек и удобство интерфейса радует глаз



ARCPR в действии - пароль найден!

софтина - вечный рулез, счастье хацкера, мир во всем мире, free Kevin now и все такое.
Качать тут: www.xakep.ru/post/13379/

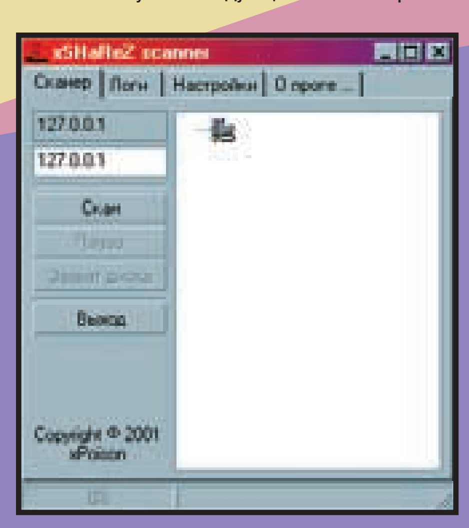
Номер раз: сканим сеть

Те, кто регулярно читают][, уже прониклись всеми тонкостями сканирования сети - будь то локалка или iNet. Сканим мы с тобой, естественно, ресурсы, доступ к которым (намеренно или по ошибке) открыт для всех снаружи, т.е. шАры (шарЫ сканить не надо). Как сканить - понятно, это дело нехитрое: запустил софтину, ввел диапазон айпишников, жмякнул пимпу "scan" и сиди, работай над собой. Любой юзер, имеющий X#1 за 2001 г., справится. Однако для начала эту софтинку нужно поиметь (я имею в виду - достать и скачать, а господина Бивиса со своим обкуренным приятелем Батхедом, которые хихикают при слове "поиметь", я бы попросил удалиться). Поэтому не буду оригинальным, если скажу, что для своих корыстных целей я, как и все нормальные люди, использую релиз журнала, прогу X-ShareZ, чего и тебе желаю. Самая свежая версия на момент написания эпохальной статьи - 2.0, однако я юзаю 1.3, и мне вполне сухо и комфортно. Для использования этого сканера тебе необходимо включить у себя следующие сетевые сервисы: клиент для сетей и службу доступа к файлам, иначе прога будет вопить об отсутствии NetBios'а и ругаться, что ты-де не вошел в сеть, что, в общем-то, правильно. Хотя, впрочем, эти службы установлены в маздайке по дефолту, просто особо умные перцы отключают их у себя, дабы, вместо того чтобы искать жертв, ненароком не стать жертвой самим.

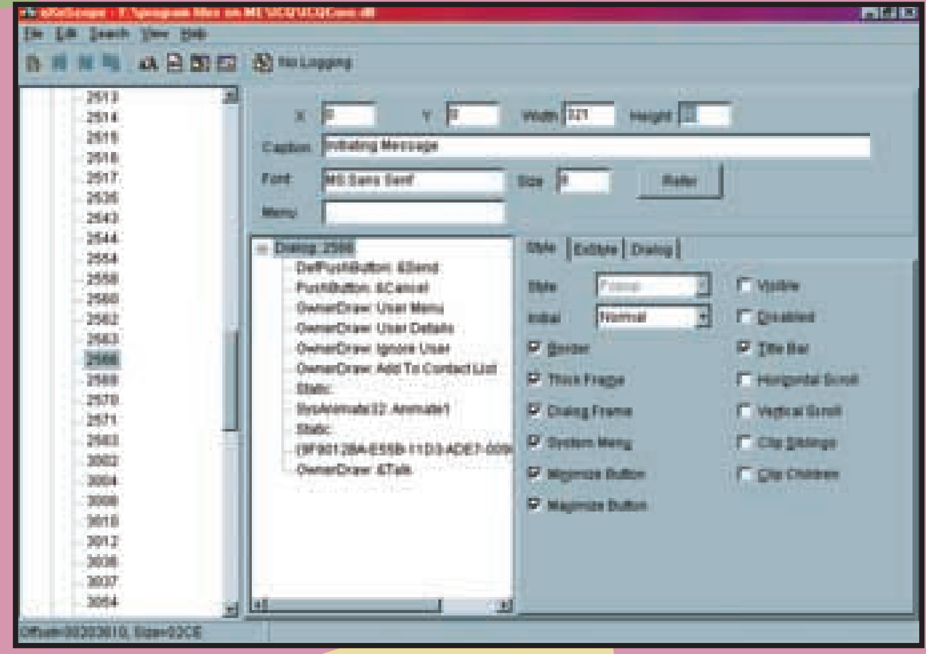
Прога написана известным челом, кандидатом в мастера спорта по художественному кодингу, хардкорным программером xPoison'ом и является настоящим][-релизом, так что если ты поклонник][, то юзать что-либо другое, кроме X-Sharez, просто моветон :). Шуткаю я, на самом деле эта архиполезная прога и без того завоевала массу поклонников, одним из которых является ваш покорный слуга. За более подробной инфой как об X-шарез, так и о шарах я отсылаю тебя к январскому номеру][за этот год.
Сливается все по адресу www.xakep.ru/post/11565/



X-Sharez by xPoison released by][



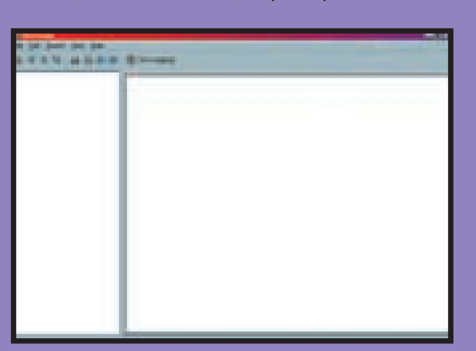
Щас будем сканить!


eXescope в действии, или Баннеры маст дай!

Номер два: разрываем проги

Многие недальновидные перцы удивляются, для чего вообще существуют такие вещи, как редакторы ресурсов. Шаровару с их помощью не сломаешь, восклицают они, а раздирать exe'шник или dll'ку только ради того, чтобы вписать в заголовок окна проги что-нибудь типа "released and cracked by kewl hacker Vasya. Yo!" или изуродовать всю геометрию интерфейса проги, это, конечно, прикольно, но не более того. Но на то они и недальновидные - правильные чуваки, вроде нас с тобой, конечно, знают, что редактор ресурсов - это вещь, а хороший редактор ресурсов - это вещь вдвойне. И уж мы найдем им применение. Поэтому я рекомендую весьма популярную прогу - редактор eXescope, версия - 6.0.

Эта софтина умеет делать все, что требуется от приличного редактора: аккуратно вскрывать файлы с расширением exe, dll, ocx, vbx и раскладывать их содержимое по полочкам: заголовки, файлы экспорта и импорта, а также самое вкусное - ресурсы файла: так выдираются, заменяются и впихиваются обратно всяческие картинки и иконки, а подвергнутая подобной обработке прога принимает неповторимый эксклюзивный вид. Ты спросишь, как же можно еще использовать eXescope? Приведу простой пример: несколько месяцев назад, когда злобный AOL решил навешать в новой версии ICQ всех достающие баннеры, по Сети то тут, то там стали раздаваться стоны: "Люди добрые, мы сами не местные, поможите, кто сколько...", тьфу ты, черт, я имею в виду стоны: "Люди! Помогите от баннеров в аське избавиться, плиииз".


Девственно чистое окно eXescope

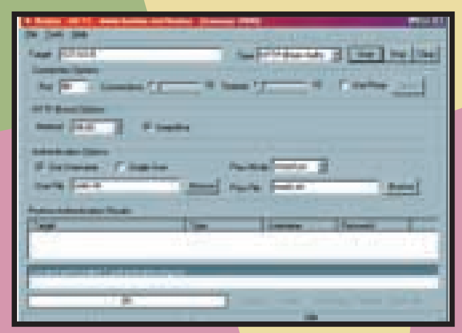
Конечно, тут же нашлись умные перцы, которые посоветовали удалить пару-тройку библиотек из аськиного дистриба, но после этой операции уродливое окно когда-то баннера все равно оставалось внизу. Нет, разумеется, сразу же были написаны и тучи прог, которые избавляли от баннера одним нажатием кнопки, но, согласись, как-то это не по-хацкерски - юзать подобные софтины. И тогда нашелся еще один умный перец, который просто запустил eXeScope, перерыл все длл'ки в аськиной папке (уже достижение, учитывая то, сколько там подобных файлов) и обнаружил, что

собака порылась в библиотечке под названием ICQcore.dll. Подправив нужный диалог и уменьшив высоту окна сообщения на размер баннера, мы забываем о навязчивой рекламе как о страшном сне - все истинно по-кульхацкерски. А ты говоришь, редактор ресурсов не нужен. А на скриншоте видно, как я навсегда избавляюсь от надоедливого сервиса в ICQ 2000b при помощи eXeScope.

И вот тебе напоследок ложка дегтя в бочку пива: я, как ни старался, не нашел официальной хоумпаги этой софтины, так что лей ее отсюда: www.xakep.ru/post/13380/

Номер три: ломаем сетевые аккаунты

Вот ты читаешь эти строки и думаешь: когда же, наконец, мы доберемся до главного: до взлома ftp и pop3 серваков, мыльных ящиков и http-форм. Что ж, ты прав, не иметь подобной проги нельзя, и я рекомендую тебе для подобных гнусных целей использовать Brutus AET2: программу, по праву снискавшую огромную популярность среди подобных себе ресурсов.



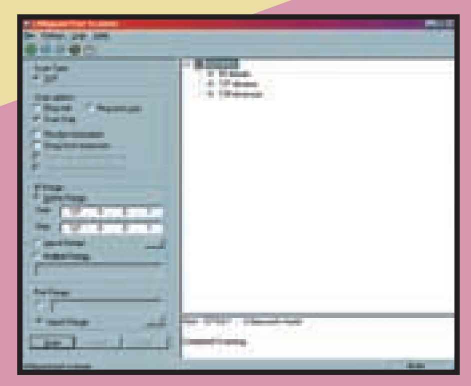
Гроза pop3-серваков и html-форм

Как ты видишь на скриншоте, чтобы юзать ее, особого ума не надо (может поэтому она так хорошо зарекомендовала себя в массах? ;). Как и во всех приличных прогах подобного рода, допускается как перебор методом беспощадного брутфорса, так и последовательный аккуратный подбор пароля по словарю. Думаю, ты не маленький, и тебе не надо объяснять, что специально к таким вот программам в Инете не составляет никакого труда найти текстовый файлик с паролями мегабайта эдак на два-три. Тебе остается только прописать путь к нему, указать мишень, на которую ты натравливаешь Брутуса (мыло, форма), тип перебора, а это может быть подбор паролей по HTTP, POP3, Telnet, FTP, IMAP, опции аутентификации (если ты подбираешь пароль к мылбоксу, то это чаще всего - логин юзверя), установить время таймаута и количество попыток, вдавить, наконец, баттон START и ждать. Время подбора пароля в основном зависит от двух вещей: от того, какой сложности пасс у юзера (если это что-то типа qWm76$#0aN*, то можешь смело забить на такой способ получения пасса), и от того, с какого канала ты ведешь перебор: на диалапе, конечно, далеко не уедешь. Хотя я знаю перца, который оставляет прогу на ночь и идет спать, а на следующий день, при хорошем раскладе, ему остается только прихлебывать утренний кофе и деловито разгребать логи. Говорят, особенно резво Brutus расправляется с так называемой HTTP Basic Auth - стандартное выползающее окошко к запароленной части сайта, где требуют ввести логин и пасс. Подробнее о Брутусе писали в][за октябрь'Y2K, статья "Грубая Сила". Надо ли говорить, что софтина поддерживает сохранение сессии, фриварна, проста в использовании, а слить ее можно прямо отсюда: www.xakep.ru/post/10763/

Номер четыре: сканим порты

Еще одна классика жанра - сканеры портов под Win32. Вот уж где самая неблагодарная работа - рекомендовать портсканер, ибо наплодилось их сейчас... Да и в][они упоминались не раз и не два... Но я все же попытаюсь привить тебе любовь к тулзе под названием LANguard port scanner, или, проще, LANScan.

Почему именно LAN Scan, спросишь ты? А почему бы и нет, отвечу я :). На самом деле, для меня определяющий фактор - это удобство и отсутствие абсолютно ненужных наворотов. Выбрал тип сканирования, настройки (пинг и/или скан),

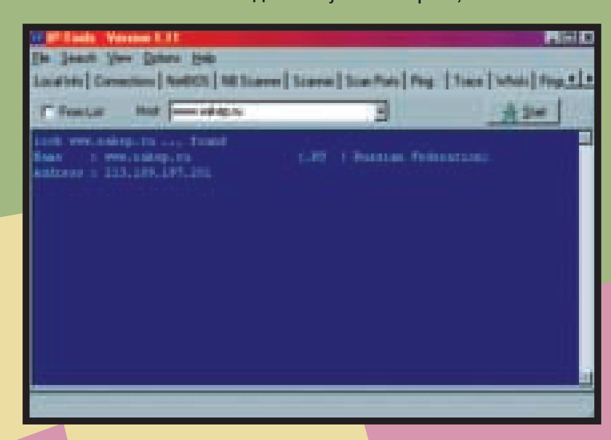


Вау, да у чувака три порта открыты. Кто же это?

ввел диапазончик айпишников, выбрал порты - и понеслась! Что тут болтать-то? Интерфейс - удобный, управление - простое, работа - надежная. Прога фриварная, сливается отсюда: www.xakep.ru/post/13381/

Номер пять: работаем с серваками

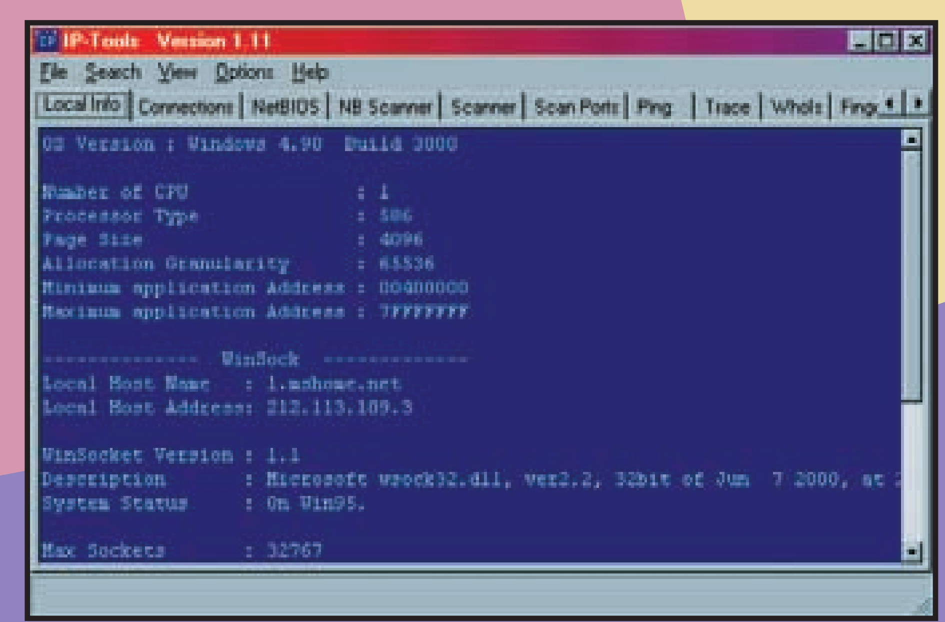
Иногда приходишь к выводу, что многие программы зазря занимают место на твоем винте: вместо того чтобы иметь десяток убогих софтин,



И никакой ты не ксакеп.ру, а всего лишь 213.189.197.201

выполняющих каждая свою одну функцию, хочется иметь одну, но серьезную прогу, которая позволит тебе использовать сетевые сервисы на все сто. У меня такая программа есть, я в ней души не чаю, а зовется она IP-tools и, вообще говоря, достаточно известна. На тот момент, когда я писал эти строки, последняя версия - 1.11.

Эта рулезная софтина имеет пятнадцать различных утилит для работы с TCP/IP-сетями. Только послушай: Local Info - инфа о твоем компе, Connections - текущие соединения твоей машины, NetBIOS - инфа о сетевых интерфейсах неприятельского компа, NerBiosScanner - подобие сканера расшаренных ресурсов удаленной машины, Portscan, Ping - ну это понятно, сканирование портов и запрос а-ля "ты жива ль еще, моя старушка?", Trace - обыкновенный роутер, отслежи-



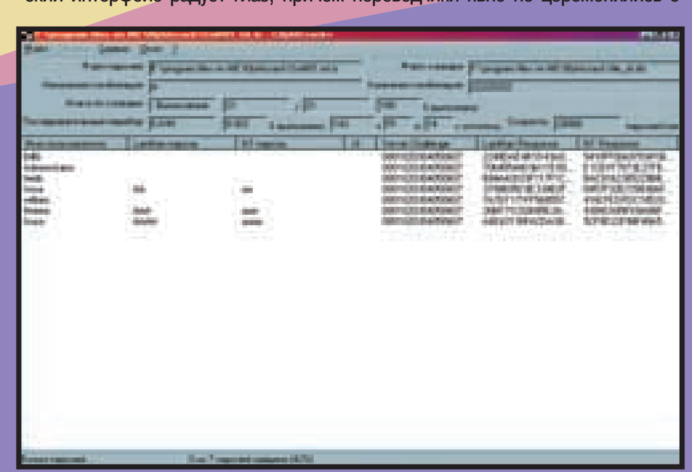
Прога с большой буквы

Двухсотпятидесятидолларовая L0phtCrack:
Дайте мне ваши hash'ики!

вающий, как пакеты летают от тебя и к тебе, WhoIs - запрос об интересующем тебя домене, LookUp - инфа об имени хоста и его алиасах по одному айпишнику, Telnet - встроенный Телнет-клиент, IP Monitor - показывает статистику отправленных/принятых пакетов, Hosts Monitor - пингует хосты и выдает на-гора их статус... Ты еще не устал? В общем, прога что надо. Я думаю, вывод налицо: зачем юзать сотни мелких, убогих по функциональности прог, если можно качнуть IP tools и наслаждаться жизнью. Качать отсюда: www.xakep.ru/post/10587/. Регистрация стоит 19 зеленых рублей, но специально для граждан exUSSR - всего девять. Е-мое, софтина того стоит!

Номер шесть: потрошим пароли

Подбирать пароли к удаленному компьютеру, конечно, хорошо, но неплохо бы и о своих, локальных паролях "позаботиться" ;). Если тебе не терпится заполучить все аккаунты в твоей локалке под WinNT, то для этого существует тулза под названием L0phtCrack+, она фриварная. Так что смотри, не перепутай ее с LC3 (тоже L0pht crack, но за 250 грин :). LC+ - это аналог шароварной LC3, служащей для взлома паролей Windows NT/2000 путем все того же брутфорса. Прога выдирает хэши паролей из удаленной машины, а затем их расшифровывает, выдавая милый взору каждого хацкера логин и пасс. Важное замечание: пароли можно взламывать, даже если Винде активизирована прога SYSKEY (а в win2k она по дефолту активизирована). К сожалению, за несколько дней до того как я сподвиг себя к написанию этой статьи, мой любимый "винтукей" накрылся медным тазом, так что запустить в сто первый раз LC3, дабы сделать тебе "рабочие" скриншоты, я не смог, а win2k-сетки у меня дома нету :).
Бесплатный аналог LC3, как я уже говорил, зовется L0phtCrack+ и распространяется свободно, при этом к тому же еще и локализована, так что родной русский интерфейс радует глаз, причем переводчики явно не церемонились с



L0phtCrack+ in action!

HIEW: под старый добрый ДОС...

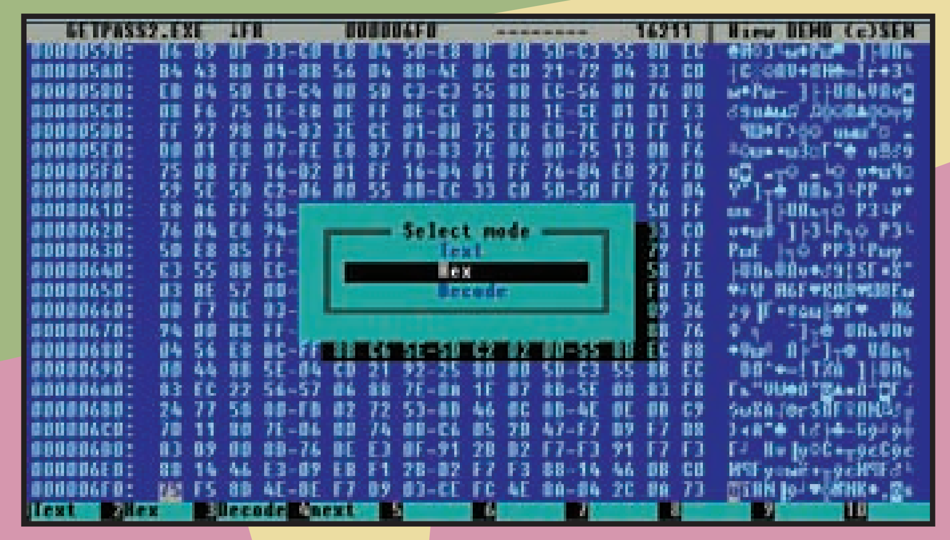
тем, как будут юзать ее софтину: если официальная LC3 на сухом языке шинели зовется "Программой для аудита и восстановления паролей Windows NT", то LC+ просто и ненавязчиво предлагает тебе свою опцию: "начать взлом паролей" :). Знали люди, кто будет юзать их тулзу.

Все это чудо сливается: LC3 - www.atstake.com/research/lc3/, L0phtCrack+ - www.xakep.ru/post/10362/.

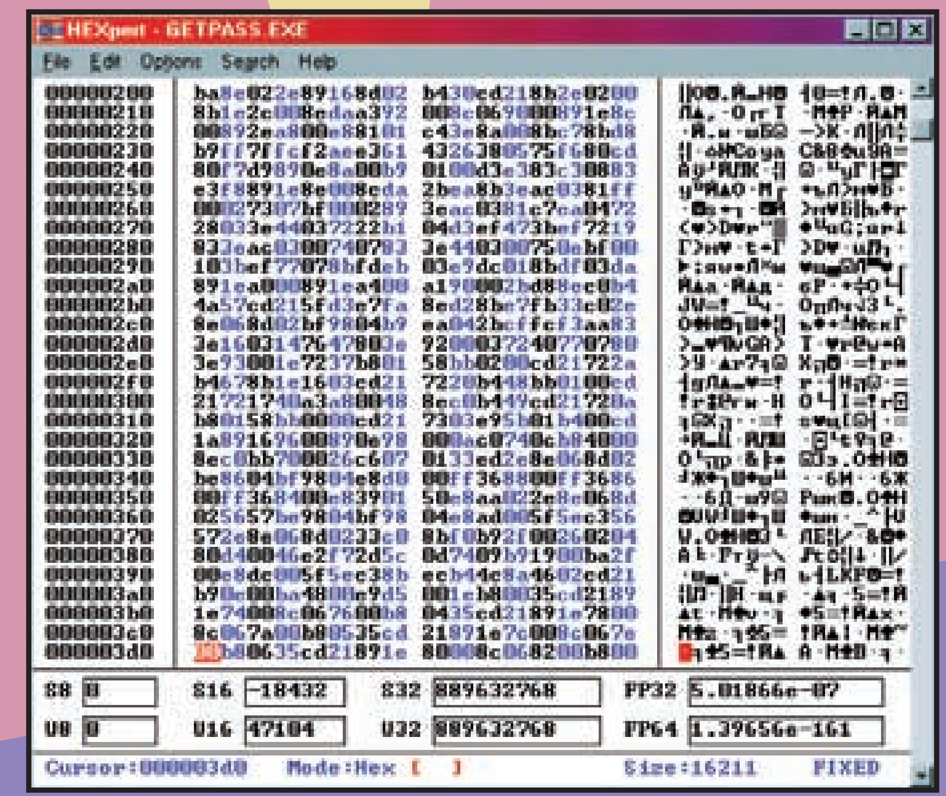
Номер семь: косим под крякеров

Последним номером нашего маленького обзора идут истинно крякерские софтины. Нет, рассказывать об основах ассемблера и расписывать достоинства SoftIce'а я, конечно, не буду - мы же с тобой не кул-крякеры, нам тяжелая артиллерия не нужна. Так, изредка во внутренностях проги покопаться, байтик-другой исправить. Что для этого, помимо дизассемблера, нужно? Правильно, шестнадцатеричный редактор, в простонародье - ХЕКС-эдитор. Популярных редакторов не так уж много, и рулят здесь до сих пор (кто бы мог подумать :) софтины под ДОС. Лично я всем им предпочитаю HIEW, тем паче, что название этому редактору дано не просто так - это аббревиатура фразы Hacker's View, хотя писал его наш, русский человек. Что мне нравится в HIEW, так это то, что он позволяет открывать файлы в формате текста, HEX-формате или в режиме дизассемблера и там же их редактировать, так что все, как говорится, под рукой.

Помимо HIEW под Винды существует еще шестнадцатеричный редактор HEXPERT, мне он нравится своим удобным интерфейсом: все регистры и адреса отмечены цветом, так что картинка получается весьма наглядная, однако в нем нет встроенного дизасма, что предполагает постоянное переключение между ним и какой-либо специальной прогой, например, Win32dasm. Да и писался он в незапамятные времена, еще под Win 3.1, поэтому не удивляйся отсутствию поддержки длинных имен файлов.



HIEW представляет: кишки exe'шника наружу



Редактор другой, кишки те же...

Если тебе, как и мне, еще очень далеко до гуру крякинга, но ручки уже чешутся, то могу посоветовать сайт http://pilorama.nm.ru - там ты найдешь много документации по взлому прог, специальные упражнения и т.д. А вообще, помню, я в свое время делал следующий финт: писал прогу, которая требовала ввести пароль, который брала из отдельного файла, и если он был верен, то радостно "подтверждала авторизацию" (кишки проги ты видишь на скринах хекс-эдиторов), а затем пытался сам же ее сломать. Метод, конечно, чайниковский, но было забавно, рекомендую тебе тоже попробовать. А проги ты найдешь тут: HIEW (на момент написания - свежая версия была за номером 6.70) - www.xakep.ru/post/10905/, HEXPERT - www.xakep.ru/post/13382/.

Если б я жил в буржуинии...

Разумеется, приятель, ты понимаешь, что ни за какую из скачанных прог ни я, ни ты платить не собираемся. Так уж повелось, что Асталависта нам роднее, чем почтовая квитанция или кредитная карточка. Но интересно, а что бы было, если б мы жили все такие из себя честные и пользовались только лицензионным софтом? Посмотрим на примере представленных мною программ.

Из них шароварными являются: ARCHPR - 60 нерусских рублей, HIEW - 10 тех же самых бумажек, L0pht Crack - 250 бакинских (Вау! И покупают?), IP Tools - 19 зеленых (для нас с тобой - девять) и, наконец, X-Sharez - 200 родных, деревянных рублей :). Дави пуск -> программы -> стандартные -> калькулятор и считай. Итого мы "сэкономили" 400 баксов, считая дорогущую LC3, или $150 - без нее. Вместо этого мы пару раз сползали на Асталависту и потратили около семидесяти рублей, купив этот номер Х, который ты в данный момент держишь в руках. Так что поднимем бокал за здоровье мирового пиратства, как бы кощунственно это не звучало. Да шучу я, конечно, шучу.

Shox R4. Пользуясь случаем, выражаем благодарность вафельнице и собакам, которые гоняются за автомобилями. Фильму про каратистов, Мерфи и его закону, бесплатному проезду, природе того и этого. Холмам, дороге, склону, тропинке, трассе и разносчику пиццы. Умению найти противовес. Греческим богам, американским горкам и будильнику. Тому, что ты знаешь, тому, чего не знаешь, и всем тем, кто когда–нибудь спрашивал почему. За и против, приливам, китайской лапше и запаху мокрой травы. Легкому весу, тяжелому весу, экстремальным ситуациям и прочему, что сделало все это возможным. Высокомерию, самомнению и зубной пасте. Дарвину и тем, кто сам завязывает шнурки. Твоему настоящему, а не прошлому, пульверизатору, поезду и не только. Дурацкой ухмылке и обезоруживающей улыбке. Тем, кто придумал субтитры, грибы, золотые зубы, ниндзя и музей. Чему–то из ничего, всему, что имеешь, твоему умению довольствоваться малым, не имея многого, и Жанне Д'Арк. Круглосуточному видеомагазину, людям, готовым говорить о том, что было, и китайским печеньям с предсказаниями. Любому, кто переступал черту, никогда и всегда. Букве, слову и свободе послать все ко всем чертям. Лестнице, лифту, такси и любому, кто прошел путь до конца. Пульту дистанционного управления, безделью, коммерческому каналу, как и для чего. Той девушке в автобусе, взглядам: вскользь, внимательному, пристальному. Попытке, неудаче и бесконечным переживаниям. Лучшему и худшему. Эго, удостоверению личности, неиссякаемой вере, потоку твоих мыслей и большой кровати. Воспоминанию о том, чего никогда не было. Дезодоранту, предлогу, планете Земля и первому, кто увидел звезды. Банкоматам, супермаркетам и фруктовым деревьям. Знаку STOP, придуманному, чтобы отдыхать. Некоторым животным (ведь ты знаешь, кто ты такой и где бегал). Изобретателю мяча, кольца, ракетки, клюшки, кия и пухового одеяла. Мужчине, женщине и ногам, которые любят бегать, и местам, куда ты идешь. Реальности, истине, духу противоречия, дождливым дням и несбыточным мечтам. Тем, кто писал правила, тем, кто их нарушал, и всем тем или всему тому, что когда–либо нас вдохновляло.



товар сертифицирован.

Телескопом по монитору, или комп - друг астронома

Трособергер-Затейник ака Mr.False(mr_false@xakep.ru)

11 июля 2001 г., 00:10... Сижу жду... Минут через сорок на юго-востоке должна появиться некая Helix Nebular, она же NGC 7293 - самая ближайшая к нам туманность. 400 000 световых лет как-никак. Времени - уйма. Может в Халву с Шлунхелем по модему рубануться, пока жду?Ах, ладно! Сам знаю, что ничего сегодня не увижу - все небо в тучах. Хотя не беда! Я эту туманность еще отследить успею! Благо, рассчитать ее появление - дело пяти минут.

Ты думаешь, я астроном/астрофизик какой, раз за туманностями гоняюсь? Ни фига подобного! Я этими штуковинами в свободное время балуюсь. А рассчитать все это дело может любой нормальный чел, имеющий комп и отсутствие кривых передних конечностей. Об этом, а, вернее, о прогах, которые позволяют проводить такие финты на компах, сегодня и пойдет речь. Итак, встречай...



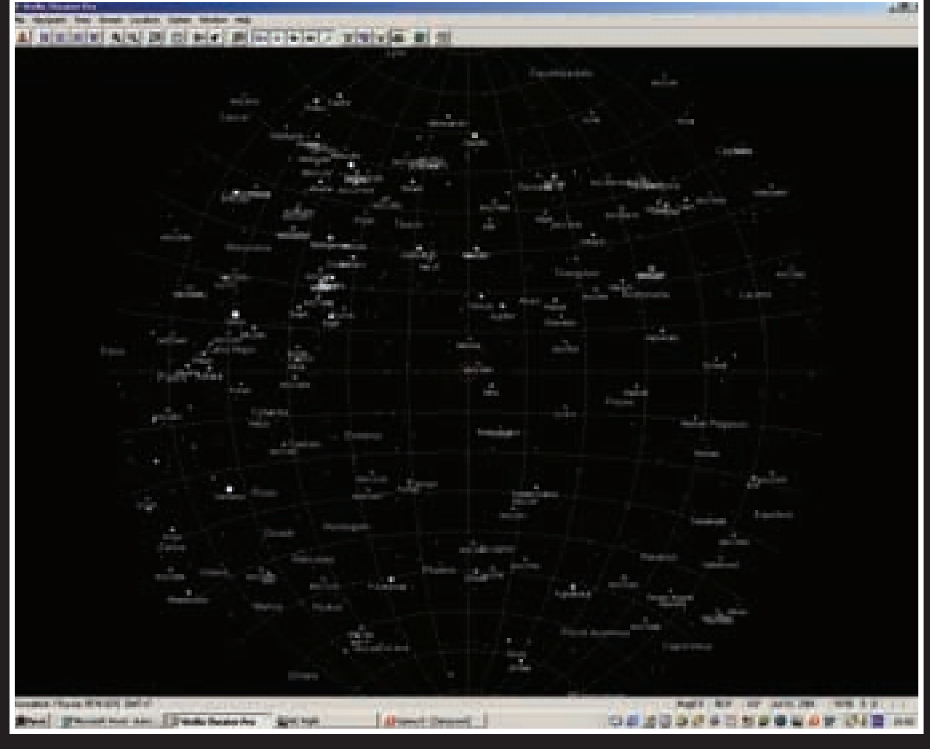
Пресловутая Helix Nebular

Stella Theater Pro v1.53

Тип: *Shareware*
Весит: *1.4Мб*
Где слить: *www.cvc.org/astronomy/spr153e.exe*

Практически ничего лишнего в данном продукте нет, хотя и некоторых весьма полезных фишек тоже нет. Основные функции, как смена места наблюдения, смена времени и анимация, конечно же, присутствуют. Доступ к ним лежит на поверхности, поэтому не приходится долго выискивать по всяким менюшкам и окошкам, где же там хату родную выбирать. Жаль только, нет слежения за временем, поэтому периодически приходится нажимать Ctrl+N, дабы обновить экран. Порадовало присутствие полноэкранного режима. Ах, как приятно на экране вместо виндов увидеть ночное небо. Особенно красиво получается, если включить анимацию - хоть screensaver делай! К вопросу о месте наблюдения: большинство крупных российских городов там тоже, как это ни странно, имеется. Каково же было мое удивление, когда я обнаружил в списке родной Новосибирск! Правда, я не понимаю, кто же делал енту программулину, если вместо привычного Moscow там пишут Moskva ;).
(Прим. ред.: буржуев в школе ничему не учат. В NeoTrace, кстати, тоже Moskva написано. Хотя, может, все и наоборот! Теперь не мы учим английский, а они учат русский :))

гони бабло или не любуйся некоторыми звездочками. Как и во всех остальных прогах - имеется настройка линии горизонта, объекты ниже которого будут не видны, но, в отличие от остальных, выполнен горизонт не то что бы красиво, а так, что просто не режет глаза. Несколько попортило



Вот оно какое - небо...

Со временем тоже имеются "небольшие" глюки: почему-то при нажатии кнопки "Get Now Time" год становится 2901-м. Я, типа, почти тысячу лет назад умер, вы хотите сказать? Для любителей астрологии эта прога может показать очертания созвездий, я такими штуками не увлекаюсь, посему эту функцию сразу отключил. Можно также вести наблюдение за каким-нибудь объектом, привязав вид к нему (правая кнопка->Set Chase). Также присутствует изменение минимального значения яркости звезд, то есть ты задаешь некоторое число-коэффициент яркости, а светила, которые тусклее данной величины, не будут отображены. Правда, ввиду того, что прога Shareware, на эту величину наложено ограничение, так что

впечатление от проги полное отсутствия в ней так называемого календаря событий, то есть, к примеру, отслеживать восход и закат наблюдаемого объекта приходится самому. Хотя для этих целей можно воспользоваться и другой программулиной. Напоследок хочу заметить, что ТОЛЬКО в STP звезды имеют цвет, который определен РЕАЛЬНЫМ спектром волн, излучаемых звездой, причем сделано это еще и в зависимости от РЕАЛЬНОЙ яркости звезды. Благодаря этой небольшой фишке рабочий экран Stella Theater Pro больше, чем у остальных прог, похож на то небо, которое мы наблюдаем ночью. Итог: самая красивая и удобная прога, хотя и лишенная некоторых полезных фишек.

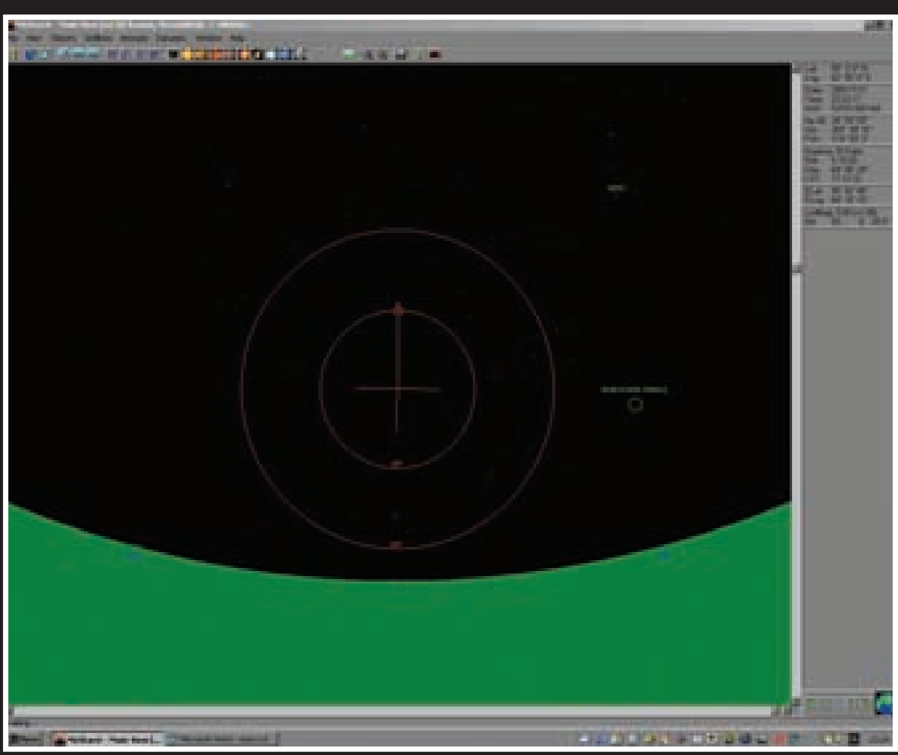
My Stars v2.7

Тип: *Shareware*
Весит: *1.4Мб*
Где слить: *ftp://ftp.sunet.se/pub/simtelnet/win95/science/myst3227.zip*

ЭТО попало ко мне на винт вторым по счету. Сей продукт менее неудобен, хотя и профессиональнее, чем предыдущий. Каждый раз при запуске ненавязчиво сообщает, что данная бойда - шароварная и луну показывать не будет. Ой, напугали! Вот если бы она туманности отказалась показывать... Следом же идет окошко, в котором просят выбрать дом родной. В списке с успехом обнаруживаются крупные русские города. Если ты вдруг не обнаруживаешь в списке своего жилища, то изволь - вводи координаты (то же, в принципе, относится и к другим программам). Присутствует стандартная функция центрирования и привязки на выделенный объект; в toolbar'е имеются даже кнопки для наведения на планеты, Солнце и Луну, которой, кстати, в проге нет ;).

ласть. А под линией горизонта расположена некая зеленая плоскость, которая режет глаза. Хотя при включении эффекта смены дня и ночи и режима анимации выглядит весьма добротно.

Пару слов об объектах. База данных несколько шире, нежели у STP. My Stars, например, показывает помимо крупных планет еще и астероиды с кометами. Если астероидов в Stella Theater Pro не было вовсе, то база данных по кометам ограничивалась тремя штуками. Поиск в MS смастерен более удобно, чем в STP. Сортировать далекие объекты (Deep Sky Objects, они же туманности и галактики - мои любимые ;) можно как по имени, номеру Messier или номеру NGC. Порадовал также тот факт, что при нажатии на какой-либо объект возникает окошко с краткой инфой о нем, в том числе и информацией о времени восхода и заката объекта! Рулез! Проблема, которая имела место быть в STP, мигом отпадает. Итого: прога с наибольшим количеством полезных фишек. Нечто среднее между профессиональным и любительским продуктами.



My Stars

Как всегда, наведение на объекты дает наилучший эффект при включении анимации, но того, что было у Stella TP, ей, пожалуй, показать не удастся ввиду отсутствия описанной выше фишки: здесь все звезды имеют одинаково белый вид, который, благо, хоть немного различается по яркости. Непонятно, зачем присутствует эффект мерцания звезд. Ребята, вы чего? На вид - почти профессиональный продукт, а туда вставляют такие, прямо сказать, детские вещи. Тем более, что на реальное мерцание все равно не похоже. Ну да ладно, зато присутствует эффект смены дня и ночи. И в довесок - реальный физический эффект преломления лучей, который как бы смещает линию горизонта на пару пикселей вниз, увеличивая этим видимую об-

Deep Space v5.56

Тип: *Shareware*
Весит: *1.4Мб*
Где слить: *www.lanet.lv/ftp/simtelnet/msdos/astronmy/dspac556.zip*

Честно говоря, не понятая мною прога. Первое, что отличает ее от остальных, - это то, что она написана под DOS (да еще и использует древний egavga.bgi!) Не понравилась немного кривоватая установка. Хотя, если внимательно следовать тому, что пишут на экране, то ставится вполне нормально. Что касается самого продукта, то он, судя по количеству настроек (смысл большей части которых до меня так и не до-

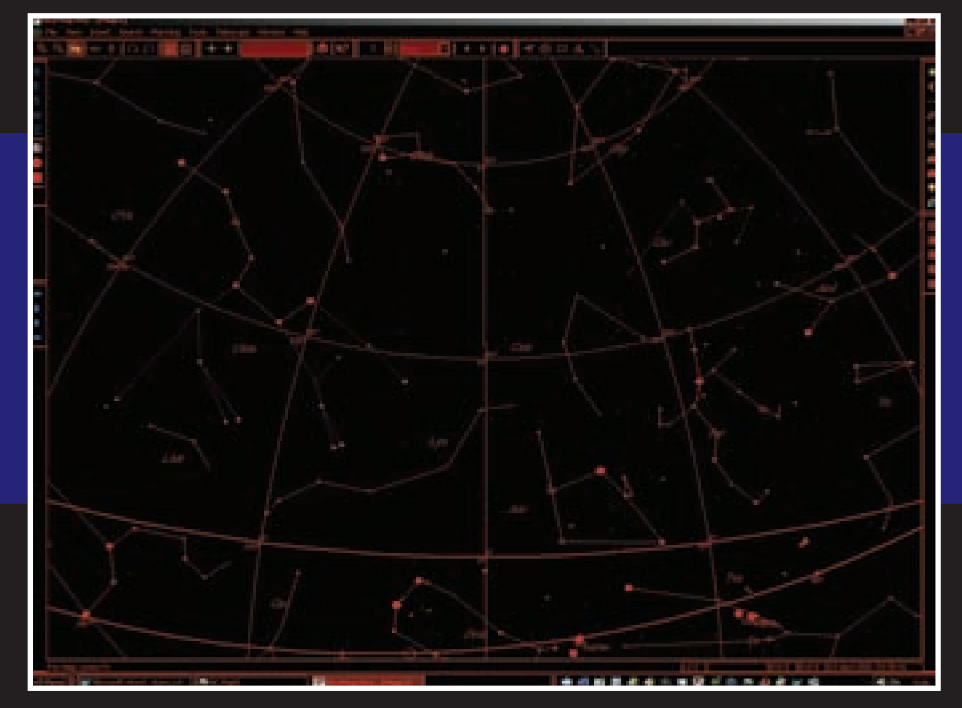
Пресловутая Helix Nebular

шел), является достаточно профессиональным. Как всегда, можно настроить время и место. Но... Во-первых, не пытайся найти в списке свой город: там городов в принципе НЕТ - только обсерватории всякие, так что вводи координаты вручную. А во-вторых, анимации там тоже нет, следовательно, чтобы отследить какой-либо объект, придется выходить и изменять время. Возникает вопрос: а на хрен это вообще надо? Отвечаю: в проге имеется такая весьма полезная для некоторых счастливых перцев фича: поддержка незаменимого в хозяйстве внешнего ТЕЛЕСКОПА, который подключается к COM-порту!!! Супер! Жаль, я не обладаю таким девайсом, поэтому, если у тебя он есть, очень прошу: поделись мнением, что это за рулез такой. А при отсутствии девайса прога - лажа. Даже не смей качать. Ну, о рабочем экране и интерфейсе тоже можно сказать пару ласковых. Тормозит. Сильно тормозит. Жутко тормозит. Даже на моем 650-м (и это - под DOS в 1998 году??). Хотя... Это ведь egavga.bgi. Все ясно, поэтому и не сделали анимацию. Интерфейс. Предельно прост, но так же предельно неудобен. Бесит, к примеру, все время давить комбинации F3-F1 и F3-F3 для простейшего zooming'а. Хотя чего я все время ее ругаю. Достоинства тоже есть. Эта прога - единственная (кроме, пожалуй, RedShift), которая показывает Млечный путь. Мелочь, а приятно. Хотя ситуацию это не спасает. Результат: прога для счастливых перцев с агрегатом ;).

SkyMap Pro 7

Тип: *Demo (Нет, не демки и интры, а демо-версия :)*
Весит: *Аж целых 9.5Мб*
Где слить: *www.wwsoftware.com/public/smp7demo.exe.*

Сразу скажу: данный продукт издается на сидюках, а через iNet доступна только его демо-версия. Прога достаточно серьезная, поэтому тратить время на геморрой с ней я тебе не советую. Тем более лить почти десять метров... Хотя, если у тебя имеется агрегат, описанный выше, то смело начинай качать. Авось пригодится (поддержка присутствует). А если девайса у тебя нет, то можешь читать дальше. Да, время, место успешно меняются. Да, есть анимация. Да, есть даже календарь событий (это реально круто). Да, есть даже поддержка ролика у крысы. Но окончательно выводит внешний вид. Ребята, если это - ночное небо, то вы явно наркоманы. Желтые звезды на синем фоне еще понять можно, но вот красные звезды на черном (когда красными становятся еще виндовые окошечки и все остальное) и ЧЕРНЫЕ звезды на БЕЛОМ фоне - это чересчур. И даже не это главное! Главное то, что нормального режима попросту нет! Ни обилие дополнительных функций, ни обширнейшая база данных не восполнят данного бага. Нет, ребятушки, вашей прогой я пользоваться не буду. Я хочу нормальное небо, а не бред пьяного наркомана. Финиш: Нарки повсюду!! Они окружают меня!! А-а-а-а-аааа!!!



Бред...

RedShift4

Тип: *Commercial*
Весит: *целых 2 компакта*
Где слить: *MiTiNo-BazZAaR и тому подобные места*

Увы. Данную прогу, к сожалению, можно только купить (конечно, можно еще и у другана взять погонять или стырить где :), потому что никаких признаков демо-версий и подобной шняги я не нашел. Но, поверь, оно того стоит! Такого обилия функций и удобства оных я еще нигде не видел. Место, время, анимация - все это в отдельном окошечке, которое появляется в правом верхнем углу при запуске и никому не мешает. Даже в менюшках лазать не приходится. Радует еще то, что весь продукт выполнен в виде электронной энциклопедии. Имеются различные познавательные ролики и своеобразная картинная галерея, которая виднеется на скриншоте. Только вот огорчает тот факт, что прога достаточно сильно притормаживает, хотя это легко объясняется просто огромной базой данных. База в два диска - это тебе не один метр в зипе. В нее включены даже те объекты, которые никогда визуально не наблюдались, от которых только был зафиксирован радиосигнал. Кстати, ты можешь пополнить базу данных своим объектом; я на днях создал искусственный спутник Земли, который имел название "Flying syphon", и долго наблюдал, как этот спутник наворачивал круги вокруг Земли. Также в проге присутствует оригинальная функция записи видео. То есть ты включаешь режим записи, включаешь анимацию и идешь пить пиво, а по возвращении просматриваешь свежеиспеченный ролик, но уже без тормозов. Правда, до красот Stella Theater Pro RS еще далеко. Хотя и так очень неплохо - попробуй сделать очень сильный zooming на какую-нибудь планету - будешь приятно удивлен. Вывод: если ты решил всерьез заняться астрономией/астрофизикой, то бери RedShift. Выбор][, однако =).

Послесловие

Вот такие плюшки. Если ты никогда не видел неба или видел его только в клеточку, то смело качай все подряд =). Может быть, у тебя возникнет желание оторвать все-таки свое седалище от стула и выглянуть в окно. А то жизнь-то проходит мимо...

Защити свою собственность!

Ограничение доступа к файлам, папкам и разным устройствам

Horrific (smirnandr@mail.ru; www.x-c-r.com)

Я не параноик и никогда не болел манией преследования. Но, несмотря на это, я всегда защищаю свою собственность. Особенно мой труд, за который я получаю деньги. Я не хочу, чтобы какой-нибудь чел стибрил мои документы или исходники прог, а потом использовал их в своих целях.

Если ты думаешь, что тебе нечего защищать, то ты крупно ошибаешься. Комп с доступом в Инет обязательно содержит пароли. Ты же не будешь помнить все параметры соединений, когда можно создать файл и хранить все там.А Минздрав предупреждает: "Хранить пароли в файлах опасно для вашего здоровья". Но это все исправимо, если правильно защищать файлы.

Если к твоему компьютеру имеет доступ несколько человек, то защищаться нужно более бдительно. Я понимаю, что ты можешь доверять своей подруге, и она никогда не будет использовать твой приват. Но защищаться все же нужно, чтобы она случайно не испортила данные или, хуже того, не посмотрела в хистори, о чем ты болтал с другими подругами в ICQ.

Причем защищаться необходимо не только от других, но и от самого себя. За моим компьютером работают 5 человек (родители, жена, брат и я), а данные уничтожаются только по моей вине. Особенно, когда просидишь за монитором 14 часов, руки сами удаляют все что нужно и не нужно :). Если я тебя убедил, то давай посмотрим, что есть интересного в мире крутой защиты нашей не менее крутой собственности.

Boot Drive Lock

www.crashcoursesoftware.com

Я начал обзор с этой проги, потому что она защищает твой комп от загрузки. После установки Boot Drive Lock переписывает загрузочный сектор так, что он грузит сначала защиту, а уж потом ОСь. Это, конечно, хорошо, если ты не юзаешь *nix. Потому что Boot Drive Lock перезапишет LILO, и *nix ты сможешь загрузить только с дискеты.

Так что эта софтина подойдет только win-юзерам, которым "эти ваши линухи" на фиг не нужны.

Итак, когда ты запускаешь прогу, перед тобой появляется простейшее окно. В нем есть пара переключателей, чтобы включить (Boot Drive Lock Enable) и выключить (Boot Drive Lock Disabled) работу тулзы. Чуть ниже есть еще параметр: "Требовать пароль при загрузке системы" (Require password to boot system). Все. Прога проста, но работает отлично. Единственное, что может обойти прогу, так это загрузочная дискета. Но это не проблема. Ты же можешь ограничить доступ и к floppy или вообще запретить загрузку с дискеты. Примечание!!! После удаления Boot Drive Lock твой Linux сможет снова грузиться с винта, потому что Boot Drive Lock возвращает LILO на родину.

Windows Security Officer

http://members.xoom.com/winsecof/officer.html

Нехилая прога от Женьки Михайлова. Прежде чем ее расписывать, хочу предупредить, что у тебя могут возникнуть проблемы с download-адресом. В момент написания статьи существовало несколько проблем.

Во-первых, xoom.com уже переименовался в nbci.com, хотя старые адреса поддерживаются. Во-вторых, нынешний владелец халявного хостинга nbci.com стал проверять все сайты и закрывать любой warez. Меня они уже прикрыли, и Женьку может постигнуть та же участь. Так что, возможно, придется поискать прогу через www.download.com или другой поисковик. А искать нужно, потому что прога этого заслуживает.

Сейчас уже существует громадное количество прог для создания защиты в Win9x. Как видишь - таких прог целое море. Есть простые, а есть достаточно сложные. Но все они могут только обеспечивать защиту. Администрировать такую систему невозможно. Так что если ты подумал, что на основе Win9x можно реализовать нечто подобное серверу, то ты сильно ошибся.

Windows Security Officer состоит из двух утил: Security Officer и Lock Desktop. Lock Desktop помещается на рабочий стол. Когда ты покидаешь компьютер, кликни по иконке, и все заблокируется, пока ты не введешь пароль. Так что не надо ожидать появления хранителя экрана.

Конечно, лучше всего поставить WinNT/2k либо *nix и получить возможность крутой защиты всего что угодно. В случае с WinNT/2k все надо, естественно, ставить не на FAT, а на NTFS. Получишь 31337-ную защиту любого файла со всеми привилегиями, рулесами и прочей секьюрностью. НО! Признайся честно, ты - не админ. Вся эта конфигурация, настройка, постоянные апдейты и слежение за новыми багами - не для тебя. Ты хочешь работать с компом и временами использовать его как игровую приставку. Ничего плохого в этом, кстати, нет. Не всем же фанатеть от ежедневной проверки безопасности и рассказывать друзьям за кружкой пива об особенностях настройки Циски в режиме удаленного администрирования. Вот именно для таких, как ты, мы и сделали эту подборочку софта.

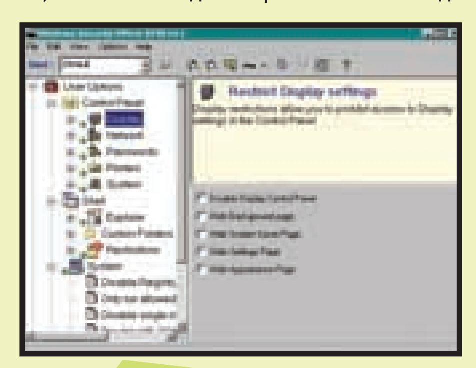
Вторая тулза - Security Officer позволяет ограничить доступ к громадному количеству параметров системы, таких как "Панель управления", "Сеть", "Настройки видео", "Принтеры". Настроек немерено, и они разнообразны. Есть такие возможности, как ограничение доступа к дискам и CD-ROM. Если у тебя к компьютеру имеет доступ несколько человек, то для каждого из них можно назначить свои настройки, т.е. создать профайлы. А главное, ты можешь указать время, в которое пользователь имеет право работать с компом. Так что Windows Security Officer наделяет твой Win9x некоторыми возможностями безопасности Windows NT.

Protector2

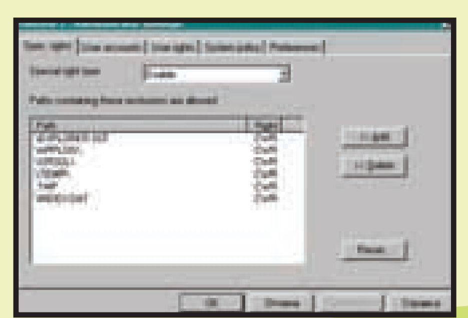
http://members.xoom.com/dolinaysoft/

Эта прога также наделяет Win9x некоторыми возможностями NT. У нее есть та же проблема с адресом, так что будь внимателен. Если Security Officer ограничивал доступ в основном к настройкам и дискам, то Protector2 ограничивает доступ к файлам и папкам. Хотя здесь тоже есть ограниче-

Boot Drive Lock



Windows Security Officer



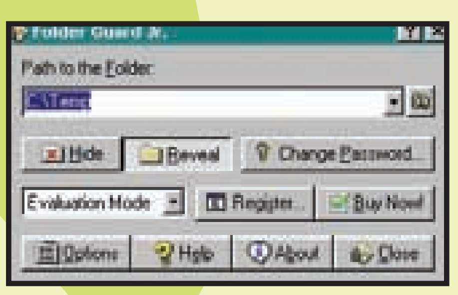
Protector2

ния, схожие с Security Officer, но их очень мало. После запуска проги перед тобой появится простенькое окно с небольшим количеством кнопок. Судя по кнопкам, возможностей мало, но стоит нажать на самую большую из них - "Admin", как ты попадаешь в другое окно, богатое настройками.
Окно состоит из нескольких закладок:
User account - на этой закладке ты можешь добавлять/удалять пользователей и назначать им пароли.
UserRights - Здесь та назначаешь права на использование папок и файлов. Для этого выдели пользователя и нажми кнопку Add. В появившемся окне ты сможешь указать папку и права на ее использование.
System Policy - Политика доступа к системным переменным. Это краткий вариант настроек, доступных в Security Officer.
Preferences - Дополнительные настройки безопасности.

Folder Guard Jr

www.winability.com/fgjr/

Очень простая и удобная прога. Она предназначена для скрытия папок от постороннего взгляда. Просто выбираешь папку и жмешь Hide. После этого никто не сможет увидеть твою собственность. Если ты забыл пароль, то для таких беспамятных есть маленькая прога Reset Password в менюшке Folder Guard Jr. Запусти ее, и пароль сбросится.



Folder Guard Jr.

Folder Guard Jr не может защитить файлы в DOS-режиме. Если загрузиться в DOS, то все файлы и папки будут прекрасно видны.

BCWipe

www.jetico.com

Прога для окончательного уничтожения файлов с винта. Ты должен знать, что при удалении файлы физически остаются на твоем винте, стирается только первая буква названия файла, и таким образом файл помечается как удаленный. Если после удаления ничего не было записано в эти кластеры, то такое файло можно восстановить (простейшим undelete). BCWipe производит окончательное удаление, затирая сектора, в которых располагался файл (этот процесс называется - wipe). После установки этой софтины при клике правой кнопкой по файлу в меню будет новый пунктик: "Delete with wiping".

PTS Strong Disk

www.PhysTechsoft.com/en/StrongDisk

Напоследок я оставил самую крутую прогу (на мой взгляд), которая обязана присутствовать в твоем арсенале. С помощью нее ты создаешь защищенный виртуальный диск, на котором можно будет хранить свои сокровенные данные. Виртуальный диск может шифроваться с помощью основных, доступных на сегодня алгоритмов шифрования: 3DES, CAST 128, SAFER, Blowfish. Для защиты пароля используются распространенный MD5 и SHA.
Несмотря на то, что виртуальный диск шифруется, он выглядит в системе как любой другой диск. Такой диск можно сделать доступным даже через



PTS StrongDisk

сеть. PTS Strong Disk прост как три копейки. В нем нет ничего сложного. В окне проги есть только две кнопки: Create - для создания защищенного диска, и Mount - для монтирования его к системе. После нажатия на пимпу Create тебе предстоит ответить на несколько вопросов, и диск готов. Виртуальные диски выглядят как простые файлы с расширением grd. Что это дает? А то, что легче осуществлять резервное копирование. А главное, ты без проблем можешь перенести этот файл на другой комп и примонтировать его там. Правда, для этого на компе должен быть установлен PTS Strong Disk.

Главный недостаток программных решений доморощенных кодеров - политика хранится отдельно от объекта. Что это значит? А то, что если ты переместишь файл, то политика доступа к нему может не переместиться. Файл может потерять все свои права, если прога не следит за перемещениями самостоятельно. Ну что поделаешь, если FAT не поддерживает нормальную безопасность. Еще один недостаток - любой сможет загрузиться в DOS-режиме и все равно получит доступ. Единственный способ обойти этот недостаток - использовать программы, поддерживающие шифрование данных.



Женский взгляд на съем в Сети

Интер-девочки и виртуальные знакомства

Александра (wantyou@yandex.ru; http://wantyou.narod.ru)

Что влечет посетителей на сайты, где большими буквами (не)известный вебмастер написал "Знакомства"? Это известно одному Богу, мне и бурундуку-насильнику Дельте.

Итак, по порядку. В Сеть, ища знакомств, по моему глубокому убеждению идут за четырьмя вещами: пообщаться и выйти в реал, пообщаться виртуально, снять партнера для секса реального или для секса виртуального. Первых большинство. Доказательств не нужно, достаточно зайти на любой сайт знакомств. Человеческая природа такова, что неуверенность в себе вырождается в уверенность в свахе, пусть даже электронной.

Любителей виртуального, именно "чисто виртуального" общения, по сравнению с первой категорией, немного. Большинство таких людей лезут в iNet из-за глубокой степени закомплексованности: в Сети он Hero, и пиктограмма у него Смерть с косой, а в реале он не более чем заштатный сисадмин, пасущий сотню-две машин, добирающийся до дома на метро, а тело его напоминает цыпленка времен застоя. Вот и остается такому человеку, заросшему непроходимой стеной комплексов, прорубать ее рассылкой писем незнакомкам. И каждый раз, когда письмо возвращается обратно, у них екает сердце, и робкая надежда корежит душу: а вдруг это та (тот), кто действительно выдержит меня без обморока минут пятнадцать в реале (достаточно, чтобы выпить чашку кофе). Хотелось бы обнадежить таких товарищей. Внешность давно не главное. И хотя симпатичность ее желательна, после первого шока начинаешь смотреть на такого человека просто как на скин давно знакомой души.

Встреча с виртуалом

Нестандартные ситуации начинают возникать, когда первая категория (желающие выйти в реал) сталкиваются со второй (виртуальными товарищами, например, мною). Возьмем пейджерное общение, например, Одигу или Асю. Стандартные три фразы, с которых начинается разговор: "Привет" (да, удивил страшно, ответ: "Ну, привет, коли не шутишь"), "Как дела?" (хм, а тебе это на самом деле интересно, отвечаю: "Пока не родила"), "Ты откуда?" (так сразу? а потанцевать? ответ разнится в зависимости от настроения). В общем, поговорили... Я ведь понимаю, что такому товарищу надо, и могу без проблем и без него продолжить разговор, задавая себе скучные вопросы: "Что делаешь в свободное время?", "На какой станции метро садишься?", "Какие пельмени предпочитаешь?", "Может, заехать за тобой?". Упс... Угадала? Бывают, конечно, товарищи, которые пытаются взять крепость с наскока. Такие рассеивают скучную и однообразную картину дня: "Тебе обязательно нужно со мной поговорить" - чем не шедевр. Хотя "Сейчас как дам табуреткой по голове... Ну, что, удивил?" - получить не слишком приятно.

Вообще, виртуальные товарищи намного интереснее в общении. Они заранее считают, что им ничего не светит и потому ничего не требуют взамен, что вполне сходит за бескорыстное общение, приятное обоим (надеюсь). Они не ле-

зут в карман за словом, им просто интересно поговорить, и они никуда не торопятся. Терпение - вот их конек. Это не то что получить письмо вроде "Такой-то, лет, рост, вес, работа, машина, дом" и в аттачменте фото на 300 кб. Наверно, считают, что чем больше фотография, тем она как аргумент в их пользу весомее. Однако ничего кроме раздражения (а все, кто пытался скачать такой аттачмент с бесплатного адреса, знают, что это такое) она не вызывает. Еще веселее получить письмо: "Ты клевая, давай дружить". Типа проходил мимо, бросил гранату в подворотню и ждет, пока рванет. Или просто фукнет. Сразу скажу: чаще фукает.

Долой буржуев!

Самые занудные парни в этом отношении - это иностранцы, помешанные на русских красавицах, которые воплощают для них недостижимый из-за пресловутой эмансипации идеал женщины. Они по непонятным причинам считают, что нормальной девушке должно быть интересно читать на четырех листах описание посещения стоматолога или получать набор фотографий с работы, с отдыха и т.п. Один турок регулярно

В Сеть, ища знакомств, по моему глубокому убеждению идут за четырьмя вещами: пообщаться и выйти в реал, пообщаться виртуально, снять партнера для секса реального или для секса виртуального. Первых большинство. Доказательств не нужно, достаточно зайти на любой сайт знакомств. Человеческая природа такова, что неуверенность в себе вырождается в уверенность в свахе, пусть даже электронной.

присылал мне сообщения по Одиге. В среднем по десять в час. Я внесла его в черный список. Тогда он переключился на электронную почту и завалил меня фотографиями (по две-три в каждом). Такое письмо весило до мегабайта, и в итоге мой ящик был пару дней блокирован, пока я не поставила фильтр. Вероятно, он до сих пор шлет мне письма, но я уже и адрес сменила. Пишу для всех иностранцев: мне абсолютно неинтересно, в каком порядке они надевают одежду утром и с каким шампунем принимают ванну, как ходит в туалет их собака и как они заполняют налоговую декларацию.

Перейдем к сексу

Тема прелюбопытнейшая. Сперва заденем столь щекотливую вещь, как съем партнера. Наталкиваясь в Интернете на массу любопытных и интересных личностей, скажу, что большая часть слухов - это просто легенды, распространяемые по причинам, лежащим в плоскости юношеского самоутверждения. Намного чаще и больше девушек (и парней) снимается в клубах и на дискотеках. Небольшой пример: мы с подружкой зашли в бильярдный клуб выпить пива. От нечего делать я стала наблюдать за происходящим. Сидят две девушки, никому не мешают. Подсаживаются парни, двое. Выпивают. Незатейливый разговор. Вроде понравились друг другу. Потом следует предложение сменить обстановку: "Что-то тут скучно. Поехали к нам...". Дальше пары снимаются с места и исчезают. За час три подобные ситуации.

В Сети подобный разговор затеять сложно. Собственно, практически невозможно. Поэтому испытывающие желание ищут других путей. Расскажу два чаще всего употребляемых варианта, которые пытается применить сильный пол. Первый: площадной вариант. Как бомбардировщики парни вооружаются каким-нибудь пейджером вроде Одиги и бомбят всех девушек, кого найдут. "Как ты относишься к сексу?" - самый безобидный вопрос. Чаще приходят такие варианты: "Займешься со мной сексом?", "Ты любишь оральный секс?". Иногда можно получить предложения и погрубее. Но приводить их не буду, пожалею бумагу. Если интересуетесь, напишите мне письмо. Что касается результатов, то за других я не ручаюсь, но я подобным приглашением ни разу не соблазнилась.

Второй, более редкий вариант. Лично я наталкивалась на такое раза два-три. Но я вообще не любитель чатов, а именно о них и пойдет сейчас речь. Горящий желанием товарищ заходит в чат, проводит там некоторое время, отбирая жертву, потом в приватном варианте отсылает приглашение весело провести время. Меня убеждали, что иногда такое срабатывает. Вероятно существуют и более экзотические варианты. Но я с ними не встречалась. Собственно, на то они и экзотические.

Скорость порождает нетерпеливость

Это в моем понимании становится аксиомой. Я уж и позабыла, когда читала российских классиков. Что касается знакомств, то большинство анкет, писем и разговоров грешит спешкой. Избыток перечислений и глагола "Давай". Как будто романтика кончилась с нажатием кнопки Power. Обидно. Хотя именно по этому параметру я определяю возраст корреспондента. Возраст пропорционален количеству разных слов.

Мы, договорясь, зашли на flirt.ru. Заняли одну из комнат и в приватном режиме предались блуду. Пальцы били по клавишам, описывая, как кто что снимает, кто что и куда засовывает и как долго там держит, как каждый задыхается от возбуждения и страсти.

До десяти - школьник. До пятидесяти - студент. Деловые люди грешат чрезвычайной самоуверенностью. Как правило, они перечисляют свои достоинства (кстати, я даже не догадывалась, что у стольких менеджеров среднего и высшего звена проблемы с половым вопросом, пока не начала получать их письма) и добавляют фотографию с собой красивым. Им, пожалуй, невдомек, что вместо того чтобы бежать к телефону,

как же, такой преуспевающий, молодой, здоровый, симпатичный, я сметаю их письма в Trash, просто потому что они невыносимо скучны: и письмо, и человек.

Виртуальный секс как он есть

Эх, вот и до виртуального секса добрались. Наверно, ты тут же представил себе кадры из фильма "Газонокосильщик". Как же! Ничего подобного. Читал порнографические романы? Текли слюни и увлажнялись полагающиеся места? Тогда тебе виртуальный секс показан. Сама я пробовала это ровно один раз. Мне не понравилось. Я чувствовала себя полной дурой и больше думала, как доставить удовольствие партнеру. Мы, договорясь, зашли на флирт.ру. Заняли одну из комнат и в приватном режиме предались блуду. Пальцы били по клавишам, описывая, как кто что снимает, кто что и куда засовывает и как долго там держит, как каждый задыхается от возбуждения и страсти. В какой-то момент я возбудилась, а потом все вдруг исчезло, и я превратилась в литературного робота. То есть для меня была перейдена грань, где кончился интерес и началась работа. Я довела дело до конца, но больше виртуальным сексом не занималась. Мне это скучно. Хотя следует признать, что у данного варианта развития отношений есть будущее.

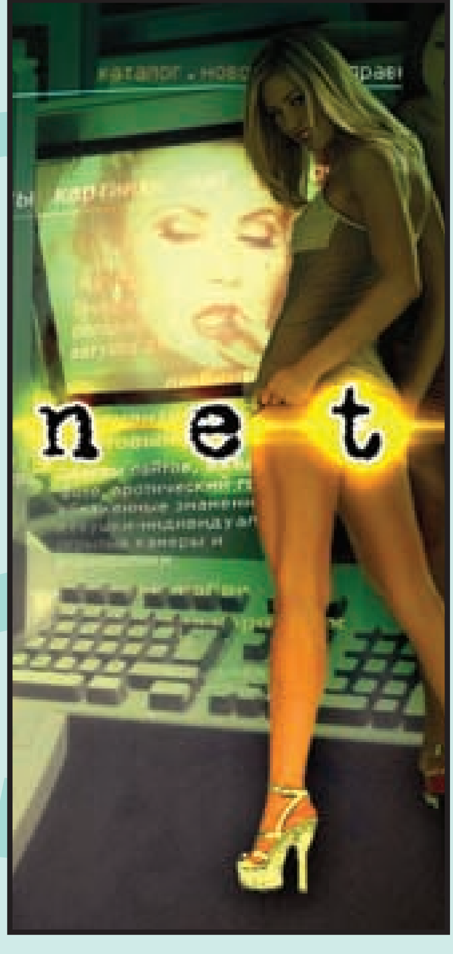
Для тех, кто дошел до этого места, я раскрою маленькие женские тайны. Скажем так, то, на что я бы купилась. Что-то на эту тему я уже писала на своем сайте, так что любопытствующие легко найдут данный материал. Здесь же я изложу свое сегодняшнее мнение по решению полового вопроса виртуальным путем.

Как надо

Прежде всего реши, нужно ли тебе это. Оглянись вокруг. Неужели рядом мало достойных внимания девушек. Ты от природы стеснителен? Ну, тогда и Сеть тебе мало поможет. Очень легко отличить по манере говорить человека опытного и того, кто пытается сделать все впервые. К последним я испытываю чувства, близкие к материнским, что вряд ли может являться хорошим вариантом развития партнерских отношений. Ищи прежде всего партнера в реальной жизни. По крайней мере, ты его видишь. Пойми, один взгляд в глаза может сказать больше, чем сто фраз в письме.

Тебе ведь интересно: бывают ли девушки в поиске. То есть занимаются ли девушки подбором партнеров через iNet. Такие встречаются, но если ты считаешь, что есть шанс, что именно ты станешь таким счастливчиком, то не заблуждайся на сей счет.

Ладно, я тебя не убедила. Тогда четко реши, чего хочешь: снять или познакомиться. В любом случае запасись терпением. Если торопишься,



то готовься приложить немало усилий. В любом случае придется потрудиться. Это как кликерные пирамиды. Только кажется, что они приносят сказочные барыши без особых усилий. Только тот, кто действительно старается, достигает значительных успехов. Если ты решил увеличить список своих сексуальных побед и не собираешься закидывать барышень предложениями заняться сексом, то слушай.

Сначала надо поговорить

Удиви девушку своей эрудицией. Не груби. Ты не представляешь, как может измениться мнение от одного неосторожно сказанного слова. Придется, хочешь ты того или нет, овладеть искусством вовремя и как бы невзначай вставить ключевую фразу насчет "где живешь" или "встретимся". Сказано невзначай, и хотя оба понимают, что это значит, но приличия вроде бы соблюдены. Можно и согласиться. Надо ли себя расхваливать? Если ты умеешь делать это с юмором, то на здоровье. Но стоит перейти на превосходную степень, то рискуешь утомить. Я тебя не вижу, поэтому не могу 100-процентно верить в то, что ты такой распрекрасный. А я, значит, какая? Впрочем, я все равно лучше. Все, разговор окончен.

Умей вовремя сменить тему

Если я не хочу говорить о чем-то, то и не надо устраивать мне допрос. Недавно один паренек пытался меня достать: где я живу, где работаю. Где, где, на планете "Земля". Так наш разговор длился около часа, но он и не сообразил, что я поговорить-то не против, но не об этом. Он просто сказал: "Не хочешь разговаривать, так и скажи." Я и сказала. Желания другого надо уважать, но не всегда им следовать.

Будь милым, но не собственником

Называй меня заинькой, но только если я не против. Казалось бы, неизбалованные вниманием девушки должны воспринимать такие слова как комплимент. А я считаю это проявлением собственничества. И ужасно злюсь. Хотя после длительного знакомства позволяю называть себя и ласкательно-уменьшительно. Пойми, что в Сети ничего кроме слов не видно. А слова - это твой интеллект. Прояви его. Я не требую решать кроссворды. Я прошу быть изобретательнее, а не давить на одно и то же. Уметь поговорить на любую тему, а не выспрашивать, где, что, как. Мне понятно твое желание узнать побольше, но прямыми вопросами этого никогда не добиться. Если то же самое начну спрашивать я, то тебе пришлось бы несладко. Можешь попробовать. Я тоже могу быть хамкой. Я могу быть какой угодно, потому я и выхожу в Сеть. Но ты можешь доставить мне удовольствие любоваться твоим умом. Тело - оно ведь вторично. Иначе его бы не клали гнить в гроб, а вместе с душой отправляли бы на небо.

Ух. Вот и все

Возможно, здесь немало сумбура. Но писать на такую тему без здоровой доли идиотизма не представляется возможным. Осталось что-нибудь добавить на десерт. Тебе ведь интересно: бывают ли девушки в поиске. То есть занимаются ли девушки подбором партнеров через iNet. Такие встречаются, но если ты считаешь, что есть шанс, что именно ты станешь таким счастливчиком, то не заблуждайся на сей счет. Во-первых, девушек в Сети не так уж и много. Большая часть - это скучающие секретарши. Они готовы поговорить, но в рамках рабочего времени. И редко сами ищут знакомств. Скорее подставляют себя и надеются на то, что их найдут. Есть еще те, кто в Сети работает. Они наиболее активны. Но ты вряд ли догадывался, что часть из них тоже ищет девушек. Да, да, не парней, а девушек. Они счастливы в браке или с постоянным партнером, а в Сети ищут удовлетворение своей второй наклонности. Упаси тебя Бог, однако считать, что активная девушка обязательно би или лесби. Избегай крайностей. Ничто не предоставляет такого разнообразия, как iNet. И здесь не может быть однозначных мнений.

Я вовсе не надеюсь, что мои советы или анализ помогут тебе найти партнера через Сеть. Я наивно считаю, что любовь обязательно должна сопровождаться божьей искрой. И даже страсть нуждается в громе и молнии, исходящих с небес. И не важно, придет это через iNet или случится в реале. Главное, чтобы сердце гулко застучало - хоть от взгляда, хоть от электронного письма в почтовом ящике.



Hi-Tech на колесах

Электроника в болиде F1

Александр '2poisonS' Сидоровский (2poisonS@real.xakep.ru)

Как ты используешь свой комп? Дай угадаю: в Инете это аська, мыло, порносайты, Каунтер-Страйк, www.xakep.ru и пара форумов по взлому? Ну, еще кряки и иногда рефераты.

В оффлайне - Word, одна-две игрушки из тех, про которые ты вычитал в нашем Зале Суда, и вечные попытки в совершенстве выучить Photoshop для оформления будущего супер-гипер-мега-развлекательного портала... Ну, может быть, что-то еще. В целом, набор стандартный, плюс-минус пара-тройка прог и сайтов.

А вот есть, вообрази себе, такие перцы, которые юзают свои компы совершенно по-другому. Нет, не Одигу вместо Аськи и Квейк вместо Каунтер-Страйка, я не про это. То есть вообще по-другому. Железо у этих перцев вшито прямо в их тачки, которые, скажем прямо, тоже слегка отличаются от привычных шестерок-девяток. Я говорю о болидах F1 и их бортовой электронике.

Случилось мне тут недавно побывать с оказией на тест-драйве команды West McLaren Mercedes на автодроме в городке Монца, что под Миланом. Прикольно: посмотрел живьем на этих монстров (в смысле, на болиды, а не на пилотов, хотя на Хакинена тоже посмотреть удалось). Шумные они, заразы - по телевизору как-то удобнее смотреть: звук потише сделал и порядок, а тут затычки в уши приходится вставлять. И вот в каждой такой дуре стоит компьютер, который контролирует все узлы машины. Во-первых, любое, производимое пилотом действие перегоняется в цифру, обрабатывается компом и затем выполняется: например, нажатие на педали, переключение передач (кстати, оно осуществляется с помощью специальных кнопок на руле) и т.д. То есть пилот жмякнул педаль, а она передает сигнал об этом бортовой электронике, ситуация анализируется, данные отправляются в офис управле-



Случилось мне тут недавно побывать с оказией на тест-драйве команды West McLaren Mercedes на автодроме в городке Монца, что под Миланом.



General Protection Error и синий экран смерти - вот и все дела. Убитый горем пилот будет вылезать из заглохнувшего болида под оптимистические сообщения типа "Если эта ошибка повторится еще раз, обратитесь к разработчику программного обеспечения".

ния гонкой, и команда выполняется (может, в конкретном примере все обстоит и не совсем так, как я описал, но смысл ты понял). Во-вторых, компьютер собирает всю текущую статистическую информацию о состоянии болида и опять же отправляет ее куда следует. В центре управления полетом :) на экране отображается доскональная инфа о машине гонщика, такая как, скажем, состояние и работа двигателя и т.д. Интересно, что во время гонки эти данные недоступны самому пилоту в болиде - никаких экранов с GUI у него нет, никакие виндоуз-шмындоуз своими окошками его не отвлекают. Да что там отвлекают - прикинь, что было бы, если б там была установлена Винда!? Ни один Шумахер до первого поворота не доехал бы! General Protection Error и синий экран смерти - вот и все дела. Убитый горем пилот будет вылезать из заглохнувшего болида под оптимистические сообщения типа "Если эта ошибка повторится еще раз, обратитесь к разработчику программного обеспечения".

Пилот жмякнул педаль, а она передает сигнал об этом бортовой электронике, ситуация анализируется, данные отправляются в офис управления гонкой, и команда выполняется.

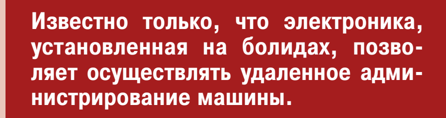
К счастью, на бортовых компьютерах F1 установлено не бессмертное творение Большого Г., а какой-то другой, специализированный софт. Какой - сие есть тайна за семью печатями, и мы раскроем ее тебе, как только взломаем базу данных хоть одной команды (если, конечно, придумаем, зачем нам это нужно :)). Известно только, что электроника, установленная на болидах, позволяет осуществлять удаленное администрирование машины (ага, это уже интересно!). То есть, например, можно дистанционно ограничить скорость болида или еще что-нибудь заподлянское с ним вытворить. Вот где настоящий простор для хакера!

Одним словом, машины F1 под завязку набиты всевозможным хай-теком, а производители прячут его друг от друга примерно как ты прячешь бумажку с паролем к Windows от своего младшего брата. На развитие электроники направлены целые лаборатории, и то, что визуально на болиде не заметно никаких компьютерообразных девайсов, еще не означает,





что их там нет. Поведение машины на трассе полностью контролируется компьютером, хотя, возможно, потрепаться в аське или погонять в Каунтер-Страйк на нем и не получится...



Известно только, что электроника, установленная на болидах, позволяет осуществлять удаленное администрирование машины.



Словарь смайликов и аббревиатур.



Стандартные смайлики

:) Улыбка
:-(Огорчение
:-) «Шучу»
[:-) Слушаю плеер
:-)~ Пускаю слюни
:-Q Курю
[!] крепко обнимаю

Предметы

\-/ Полный стакан
\/ Пустой стакан
(|||) Гамбургер

Эмоции

:-|| Сержусь
=:[] А-а-а! Ужас!
+[Маст дай!
(:-... Убит горем
:-< Плачу
;-) Подмигиваю

Как жизнь?

/:-) «Крыша едет»
:*) Пьян
%-) Пьян, но счастлив
:-/i~~ То-о-ошни-и-ит...

Аббревиатуры

1sec	wait a second	подожди секундочку
2day	Today	сегодня
2moro	Tomorrow	Завтра
2nite	Tonight	Ночью
ASAP	As Far As I Know	Насколько мне известно
BF	Boy-Friend	Любовник
CU	See You	Увидимся
CUL	See You Later	Увидимся позже
FAQ	Frequently Asked Questions	ответы на часто задаваемые вопросы
GF	Girl-Friend	Подружка
H8	Hate	Ненавижу
IMHO	In My Humble Opinion	По моему скромному мнению
NP	No problem	Без проблем
PLZ	Please	Пожалуйста
2BCon...		продолжение следует...

Fаqльтет X, или куда пойти учиться...

Александр Соловьёв aka pingWIN (a-soloviev@newmail.ru)

Отгудел последний гудок, сожжены дневники и тетради, два раза посеян и три раза найден аттестат, окончательно заблеван выпускной костюм. Думаю, многие с трудом вспоминают подробности данных событий. А ведь утром с больной головой некоторые начинают думать, куда ж все-таки поступать. Им уже не поможешь. Все нижеследующее пригодиться тем, кому предстоит пережить все это через год-два.

О ВУЗе надо начинать думать заранее, тем более, если ты еще не определился с профессией. Гораздо проще, если ты уже решил кем стать. Я, например, решил стать програмайзером еще в 11 лет. Тогда, будучи полнейшим компьютерным отморозком, я только-только прошел DUNE II и решил, что если меня и возьмут в армию, то только как главнокомандующим.

Очень полезно поступить в спецшколу при каком-то ВУЗе в классе в 9-м или 10-м или долго и упорно ходить на вечерние курсы - это все понятно. Но ведь и сам ВУЗ надо выбирать себе по силам. Далее я попробую помочь в этом будущим програмайзерам.

Сейчас многие ВУЗы готовят программистов, обещают золотые горы и кричат, что они самые-самые. Но я могу сказать, где точно реально готовят...

Московский Государственный Университет им. Ломоносова,

факультет Вычислительной Математики и Кибернетики (МГУ фак. ВМиК)

Сюда поступают только большие мозги и большие кошельки. Невозможно сдать экзамены, но учиться проще. Сдавать: математику письменно и устно (обе по 10-бальной системе), физику устно и сочинение (по 5 баллов). Сочинение и письменная математика нереальные на всех факультетах. Есть и платное отделение, но туда берут только тех, кто совсем немного недотянул до проходного балла. Куча разных подготовительных курсов на любой вкус: можно ходить, начиная с 8 класса, а можно и в последние 4 месяца. Деканат всячески отрицает существование каких-либо спецшкол или профильных классов. Специальность: “Прикладная математика и информатика”, специализации: математическая физика, математическое моделирование, вычислительная диагностика, численные методы, исследование операций и системный анализ, актуальная математика, оптимизация и оптимальное управление, теория вероятностей и математическая статистика, математическая кибернетика, математическое и программное обеспечение проблемно-ориентированных систем, архитектура вычислительных систем и сетей, математическое и программное обеспечение вычислительных машин и систем. Учиться - 5 лет.

Есть и предварительные экзамены (двухтуровая олимпиада в конце апреля), но это совсем нереально.

Люди там веселые, считай - элита (не та, что пальцевитая) - все-таки лучший ВУЗ страны. ВМиК делит один корпус с экономическим, так что попадается много красивых девушек :). Иногородним на время экзаменов даже предоставляется общежитие.

Куда звонить:
Приемная комиссия - 939-55-90
Вечерняя математическая школа, 8-11 классы (ВМШ) - 939-53-74
Подготовительные курсы (1 год или 4 месяца) - 939-54-49
День открытых дверей: в начале января и в последнее воскресенье марта.
Инет:
www.msu.ru - сайт МГУ
www.vmik.msu.ru - сайт ВМиК МГУ

Московский Государственный Технических Университет им. Н.Э. Баумана

факультет информатики и систем управления (МГТУ, фак. ИУ)

Хорошо известный (даже за бугром) ВУЗ, куча факультетов и специальностей, реальные экзамены для мозговитых перцев, но учиться невозможно. Многих выгоняют, многие сами уходят, так что халтурить вряд ли получится.

Сдавать: математику, физику, сочинение или тест по русскому и литературе - выбираешь сам. Все письменно. Задачи все типовые (то бишь похожи друг на друга из года в год), так что подготовиться вполне реально, но нужный балл на ИУ набирают в основном из профильных школ или с подготовительных курсов (самый популярный факультет, самый большой проходной бал). МГТУ имеет много профильных школ и спецклассов в обычных школах. Самая крутая из них - лицей 1580 (школа 1180). Там есть только 10 и 11 классы (10 десятых и 11 одиннадцатых классов). Школа бесплатная, но в нее еще поступить надо. Учиться трудно (весь 10 класс имеют по полной программе, а в 11-ом можно халтурить), но зато потом будет легче в Бауманском. Куча разных льгот при поступлении в МГТУ (сдавать вступительные можно будет 3 (!!!) раза).

Весной проводится платное тестирование (для профильных школ - бесплатное), по результатам которого можно поступать. Тестирование - те же вступительные экзамены по тем же предметам, но под другим названием (теперь многие ВУЗы так делают).

В Баумανском есть и платное отделение, но вряд ли найдется много извращенцев, которые будут платить за то, что их будут иметь 6 лет. Немереное количество чертежей, сопромата, стендовых д/з и т.д.
Теперь поподробнее о ИУ. Факультет зарождался еще в 1930-ых (!!!) годах (гы… Тогда они, наверно, логарифмические линейки строгали, автоматизировали, а потом управляли ими :). Есть 9 специальностей (9 кафедр):
ИУ1 - Системы автоматического управления летательными аппаратами aka kaka.
ИУ2 - Приборы и системы ориентации, стабилизации, навигации aka стабилизец, ориентец и нафигец.
ИУ3 - Информационно-измерительная техника и технология aka мастерская по логарифмическим линейкам.
ИУ4 - Проектирование и технология электронно-вычислительных средств aka ehse odna kaka.
ИУ5 - Автоматизированные системы обработки информации и управления aka soft.
ИУ6,9 - Вычислительные машины, комплексы, системы и сети (чем 6 отличается от 9, никто сказать не в состоянии) aka железо.
ИУ7 - Программное обеспечение вычислительной техники и автоматизированных систем aka soft.
ИУ8 - Комплексное обеспечение информационной безопасности автоматизированных систем aka вооруженная охрана.
Причем их можно грубо разделить на 2 направления: собственно информатика (ИУ5-9) и системы управления (ИУ1-4) :).

Куда звонить:
Приемная комиссия - 263-65-41
Справочная МГТУ - 263-65-91
Подготовительные курсы (вечерняя физико-математическая школа) - 263-66-05
Физико-математический лицей 1580 (школа 1180) - 316-59-66
Инет:
www.Bmstu.ru - сайт Бауманского
www.1180.bmstu.ru - сайт школы 1180

Московский Институт Электроники и Математики (МИЭМ)

Középненький, но достаточно известный у нас ВУЗ. Это вариант для подстраховки при поступлении в хороший ВУЗ. Поступить реально, хотя без подготовки трудно. Учиться тоже реально, а халтурить еще реальней. Куча подготовительных курсов, спецшкол, профильных классов в Москве и области (см. на сайте МИЭМа) - все как платное, так и бесплатное. На бесплатных курсах (про платные ничего не знаю) готовят очень хорошо, поэтому большинство поступивших именно оттуда. Есть курсы и для отслуживших, и для работающих, и для школьников 9-11-х классов. Сдавать математику письменно, физику устно и русский - сочинение.
Факультеты:
- электроники
- автоматики и вычислительной техники
- информатики и телекоммуникаций
- прикладной математики
- экономико-математический
- общеинженерный

Куда звонить:
УВК N1840, м. “Проспект мира” - 280-07-74
Лицей N1537, м. “ВДНХ” - 182-19-44
Бесплатная вечерняя физ-мат школа - 916-88-62
Приемная комиссия - 207-78-30, 916-88-08
Платная вечерняя физ-мат школа “Логос” - 457-65-52
Платные подготовительные курсы Центра Профессионального Обучения - 235-44-35
Инет:
www.miem.edu.ru

Академия ФСБ

Говорят, что здесь самая крутая кафедра информатики в России, хотя поступают туда только пальцевитые. Такое ощущение, что конкурсный отбор производится исключительно по должности твоих знакомых в ФСБ. Извне народ почти не поступает. Заявление о поступлении нужно подавать в местное отделение ФСБ, где тебя сначала проверят, потом пройдешь там же собеседование. Если успешно, про пройдешь “медицинское и психофизиологическое обследование” (цитата). А дальше экзамены в сам институт.
Экзамены:
На факультеты прикладной математики и информационной безопасности:
- математика (письменно) - профильный
- физика (письменно)
- русский язык и литература (письменно)

На факультет специальной техники:
- физика (письменно) - профильный
- математика (письменно)
- русский язык и литература (письменно)

Куда звонить: *инфы нет. “Юридический адрес: 117602, г. Москва, Мичуринский проспект, 70”.*
Подготовительные курсы: точной инфы нет. “Абитуриенты, проживающие в г. Москве или ближнем Подмосковье, могут поступить в вечернюю физико-математическую школу при Институте. Набор в школу производится через кадровые аппараты соответствующих подразделений ФСБ России и других министерств и ведомств без экзаменов”.
Инет: *www.fssr.ru*



Витольд Барский (http://x-books.ft.inc.ru/), Асёна (asya@ft.inc.ru)

Петровский А.И., "Хакинг, крэкинг и фрикинг: Секреты, описания атак, взлом и защита" – М.: "СОЛОН–Р", 2001

Перед тобой книга, которая сама себя называет первой российской энциклопедией по хакингу. Похоже, что так оно и есть. В книге до кучи ценной инфы - почти все, с чем может столкнуться хакер в своем нелегком труде, там есть. И про различные оси, протоколы, сетки, и про разнообразные прикладухи, в том числе шароварные, и про мыло, чаты и веб-сервера, и, конечно, всякие телефонно-пейджерные шмудацкие штучки. Особо здорово, что количество тем в книженции не идет во вред качеству, и все, в ней упомянутое, описано дельно и обстоятельно. Тут тебе и небольшой ликбез по теме (вдруг ты, перец зеленый, еще не знаешь команд юниксовых или где какая ось системные пароли хранит - все мы когда-то начинаем), и джентльменский набор хакера для ломки конкретной штуковины. Понятное дело, такие наборчики для разных дел разные. В итоге, прочитав эту книгу, ты вооружишься до зубов: у тебя будут знания функционирования различных систем, плюс ты будешь знать, где в них какие дыры, и плюс у тебя будет инструмент для проникновения в эти дыры. Ну, по ходу всей книги время от времени тебе будут встречаться прямо-таки готовенькие рецепты типа "сделай сам". То есть набор конкретных шагов, выполнив которые, ты без всякого подключения мозгов сможешь что-нибудь хакнуть. Но это вариант для полных отморозков, так как без мозгов эти твои "конкретные шаги" могут быть последними в твоей компьютерной жизни (по крайней мере лет 5 - точно).

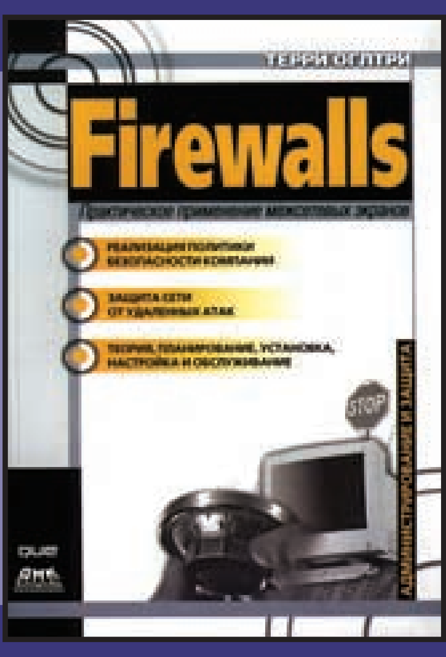
Максим Букин, Денис Букин, "Субкультура хакеров" – www.inroad.kiev.ua

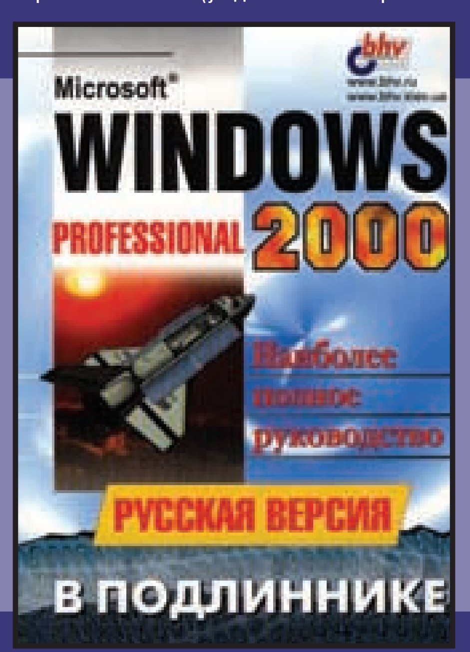
Эта книжка не похожа на остальные хакерские книги. Во-первых, она предлагается тебе не в бумажном виде, как все остальные, а полностью выложена в Инете. Во-вторых, здесь ты не найдешь ни кодов, ни описаний систем, команд, методов взломов и приемов работы с хакерскими программами, потому что книга и не про хакинг - книга именно про хакеров, их культуру, психологию, о том, как они появились, как развивались. В-третьих, при чтении книги не возникает впечатления, будто она написана каким-то иностранцем, будто это перевод - как раз наоборот, описываемые в ней реалии вовсе не кажутся сугубо забугорными. В-четвертых, в ней дан однозначный ответ на вопрос "хакер - это хорошо или плохо?" (угадай какой! или прочитай в самой книге). И все эти непохожести дают ей много плюсов.

Что ты сможешь узнать из этой книги? Прочитаешь, откуда ты, хакер, взялся - свою историю. Уверен, что по молодости тебе интереснее самому что-нибудь хакнуть, чем прочитать про историю и идеологию этого, хакерского, дела. Но олдовые челы с удовольствием окунутся в хакерскую философию и в подробные рассказы о первых хакерских атаках, громких именах и событиях, которых достаточно много в книге. Это и дела известных российских и забугорных хакеров, и взломы сайтов крупных корпораций, и разрушительные проделки всемирно известных вирусов. Ну и узнать из первых рук, от профессионалов-хакеров, ответы на разные вопросы - книга заканчивается несколькими интервью с представителями компьютерного андеграунда, которые не понаслышке знают и о взломах, и о субкультуре.

Оглтри Т., "Firewalls. Практическое применение межсетевых экранов" – М.: "ДМК Пресс", 2001

Если тебе вдруг захотелось защитить свой комп от атак через Инет, то эта книга для тебя. Если ты все еще не предохраняешься, то ты можешь только догадываться, какая куча народа пытается тебя хакнуть через сеть. Но если у тебя голова хоть немного варит, то ты уже, конечно же, фаревол поставил, а если еще нет, то уж после прочтения этих строк поставишь точно. И эта книга тебе поможет в таком важном деле. Во-первых, в ней есть обзор халявных (для настоящего хакера других и нет ;) межсетевых экранов или брандмауэров, как еще называют Firewalls по-русски. Тебе подробно опишут весь инсталл и настройку этих программ, чтобы ты мог не забивать такими мелочами свою светлую голову. И неважно, на какой оси ты сидишь, так как для каждой сможешь подобрать себе фаревол. И это, так сказать, задача-минимум, которая может стоять перед тобой при применении этой книги. Во-вторых (это уже пошло для более сообразительных челов), книга включает сведения по теории межсетевых экранов и введение в набор протоколов TCP/IP, а также описание слабых и уязвимых мест в глобальных сетях и обзоры атак и взломов. В-третьих, ничего дополнительно не устанавливая, ты можешь научиться укрепить свой комп и мониторить свою операционку на предмет атак на твой комп. Фанатикам и спецам будет интересно приложение, в котором описаны все





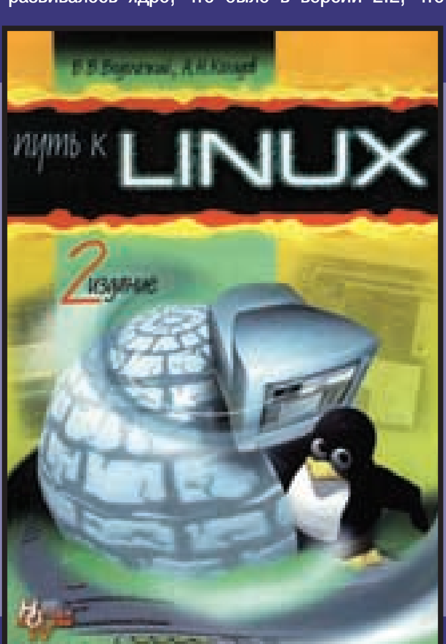


стандартные порты TCP и UDP. Короче, любой тут найдет для себя полезности.

Водолазкий В.В., Колядов А.Н., "Путь к LINUX" - Издание второе, переработанное и дополненное - М.: "Нолидж", 2001

Хочешь иметь Linux, но не знаешь как? - Купи книгу "Путь к LINUX" и ты в полной мере удовлетворишь это свое желание. Не будем кричать на каждом углу "windows must die" или "в линуксе мало приложений", а разберемся тихо и по делу. Хотя эта книга представляет, так сказать, сторону линуксоидов, но я бы предложил поюзать эту буку и тем, кто пока еще не проникся идеей, что линукс - это рулез. Потому что, прочитав ее, каждый сможет получить ответ на вопрос, нужен ли ему линукс или нет. Но ты ведь не каждый и ты, я уверен, давно знаешь ответ на этот вопрос, а я знаю, что он положительный. Итак - к делу.

Перво-наперво тебе нужно будет раздобыть линукс. В книге речь пойдет о двух дистрибутивах - Slackware и RedHat - выбирай. Большинство книг на установке и начальном минимальном конфигурировании и заканчиваются. А в этой все самое интересное и начинается. Сначала подробно объясняется, как надо сконфигурировать ядро. Затем, при желании, ты можешь разобраться, как развивалось ядро, что было в версии 2.2, что



появилось в 2.4. Ну и закончим основную установку линукса инсталлированием оконной среды - вещь важная и удобная. К твоим услугам аж шесть различных окошек.

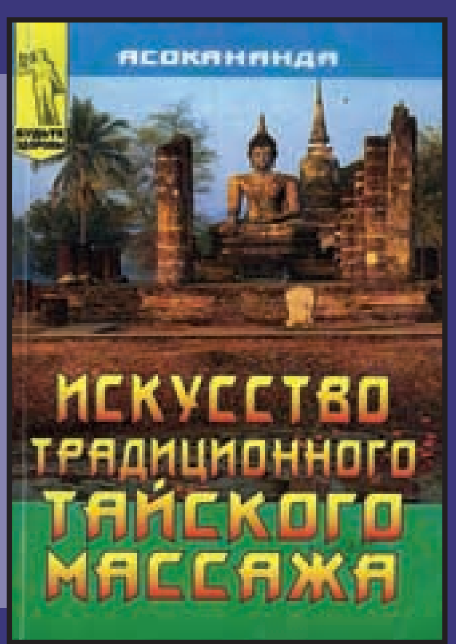
На этом можно и остановиться, но истинные хакеры, которые привыкли идти до конца, продолжат свой путь и дальше. Путь этот называется созданием комфортной среды. В этом разделе ты найдешь вопросы загрузки и разгрузки системы, прав доступа и регистрации, создание загрузочных дисков, подключение принтера, стриммера, зип-драйвов, магнитооптики и упсов. И далее - самая интересная тема для супер-хакеров: безопасность линукс-систем и защита данных. Здесь - все о том, что надо сделать, чтобы тебя не хакнули, и что надо делать после того, как тебя все же хакнули. ;-)

Что тебе еще надо? Само собой, подключить свою тачку с линуксом к Интернету (а иначе зачем все это надо было делать?). Ты установишь ppp-соединение, браузер, fpt-клиент и электронную почту, а если очень хочется, то веб-сервер апачи. Вот и все для начала. А дальше ты сам сообразишь, что делать.

Андреев А., Беззубов Е., Емельянов М., Кокорева О., Чекмарев А., "Microsoft Windows 2000 Professional. Русская версия" - СПб.: "БХВ-Петербург", 2001

А эта книга для тех, кто выбирает виндоуз. Последнюю версию - 2000. Если ты любишь все самое новое и если комп у тебя шустрый, и если ты привык в виндах работать, то эта книга - для тебя. С ее помощью ты разберешься во всех тонкостях винтукея. Начиная с установки системы и кончая вопросами обеспечения работоспособности - самым пикантным местом серии виндоуз. Не зря, наверное, в книге несколько глав отводится этой теме: восстановление системы, сообщения системы (в том числе популярный "синий экран смерти"), работа с отладчиком и работа с реестром.

Если ты когда-нибудь раньше видел книжки серии "в подлиннике", то ты помнишь, что каждая из них - толстая и умная как бегемот. И эта книга - не исключение. В нее так много поместилось, что в обзоре и не охватить. Много информации для юзеров - описание настройки интерфейса и вообще всяко-разная мелкая конфигурация, а еще диски, файловые системы и служба печати. Излишне говорить, что все темы рассматриваются достаточно подробно, с рисунками и попунктно.



Много места в книге занимает администрирование системы, которое расписано на различных уровнях: и как управление компьютером в целом, и как управление служебными програми, событиями, устройствами и юзерами. А еще больше места отводится сетевым фенечкам: протоколам, коммуникационным службам и работе в Инете. Последний момент - Интернет - особенно подробно. Здесь речь идет и о браузере (угадай, каком?), и почтовике (тоже можно долго гадать), и о службе IIS (в нее входят сервера: web, ftp и smtp).

Еще один большой раздел книги посвящен защите твоей виндоуз и инфы, которую ты хранишь. В этом разделе книги написано про безопасность как изолированного компа, так и работающего в сети. В первом случае микрософт, виндоуз 2000 и авторы книги, вместе взятые, предлагают использовать шифрующую файловую систему (EFS), работающую только на NTFS 5.0. Во втором случае - протоколы аутентификации, сертификаты и безопасность IP.

В общем, если ты делаешь выбор системы, в которой все проги одной фирмы завязаны друг на друга, про проги же других фирм ты готов забыть, то эта книга вместе с windows 2000 - твой выбор.

Асокананда, "Искусство традиционного тайского массажа" - М.: "КРОНН-ПРЕСС", 1999

"Здрасте! Я родом из Бобруйска.

Я - гуру, по-вашему это будет "учитель".

Я щас вам расскажу о смысле жизни,

Я, в натуре, профессионал, а не любитель"

Так выслушай же мои речи, отрок, и внемли ;).

Устав от многочасовых компьютерных боев, от мирской суеты, хорошо бы тебе окунуться в мир духовный. Именно в этом мире существует такое привлекательное и, казалось бы, плотское дело, как тайский массаж. Тебе, наверное, представляется ночная жизнь Бангкока, массажные кабинеты, где предлагаются услуги, о которых подумал твой возбужденный мозг. Но традиционный тайский массаж - это нечто совсем другое. Его история начинается лет 2500 назад, во времена Будды, а основателем, по преданию, считается врач из Индии Дживака Кумар Бхаши. Теоретическая основа тайского массажа зиждется на концепции о невидимых энергетических линиях, пронизывающих все тело, 10 из которых играют особую роль, - это "Десять Сен" или "Сиб Сен". С этого, истории и теории, начинается книга, которую я тебе представляю. А продолжается она описанием практических приемов, техник и стилей массажа. "Зачем это мне?" - как бы спрашиваешь ты меня. "Надо!" - как бы отвечаю я тебе. Ну, представь, прочитаешь ты эту книгу, научишься всем этим премудростям (это, скажу я тебе, не сложней, чем пароль в ворде хакнуть), научишь свою герлу - и вперед, к вершинам кайфа. Здесь я не буду особо описывать, как можно воспользоваться полученными знаниями, так как надеюсь, что твой возбужденный мозг сам тебе подскажет. Скажу лишь, что можно этот массаж применять и по прямому назначению, то есть лечить разные болячки и поддерживать свой организм в здоровом состоянии. А то много ли систем ты больным хакнешь?

*Книги для обзора предоставлены магазином издательства **"BHV-Санкт-Петербург"**, **www.bhv.ru***



Захват канала в IRC (ver. 2)

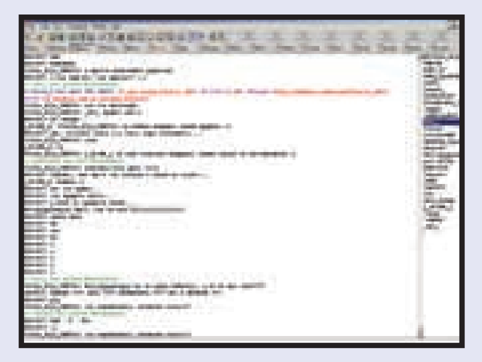
Коваленко Павел aka donRumata

Клинический случай

Туточки недавно (совершенно случайно) у своей знакомой прочитал в X статью, где рассказывалось, какие бывают виды захватов IRC-канала и зачем это нужно. Мысленно попытался представить себе автора - эдакого хакера с кучей рутовых терминалов, когда-то посещавшего IRку и теперь пишущего ностальгические мемуары. Например, какой идиот предоставит мне права на редактирование конфигурации собственного бота, если это не я сам? Естественно, для этого придется ломать сервант, где висит ботва. Это гимор, которого часто не хочется: мне же никто $ за тэйковер не будет башлять, это просто игра. Или - "запинговать насмерть". Что автор имел ввиду? Если примитивный CTCP-флуд, то всегда можно поставить скрипт даже в клиенте, который на 10 пингов в 1 секунду творит "mode +kb $chan $nick", обычно просто игнор в течение 10 минут на любые проявления ctcp/dcc/text флуда. Если же подразумевался echo ping flood, построенный на всяких smurf`ax, rapid`ax, slicer`ax, stream`ax, то… Тоже облом, ведь далеко не всякий сервак стоит на крохотном 2M-канале. Есть и индустриальные OC-12 гиганты, которые к тому же жестоко закрыты от хакерманов кучей маршрутизаторов, разбросанных по всей сети и сводящих на нет основную часть ping-based атак. Естественно, всегда найдется хитрая голова, что будет атаковать с 10 других подобных машин и добьется своего… Но так оно складывается не всегда, увы. Итак, давай вернемся в объективную реальность и отметим некоторые аспекты, блаженно забытые автором предыдущих "Захватов".

Реальность IRC-разборок

После всего сказанного хотелось бы описать реальные захваты каналов. Реальные захваты - реальные каналы. Кто они? Есть некорректные, общие признаки: висит не менее четырех ботов круглосуточно, что благополучно слинкованы между собой; хранят покой посетителя - 20 операторов, обвешанных защитными скриптами; как боты, так и опы обладают хостами, разительно отличающимися друг от друга и

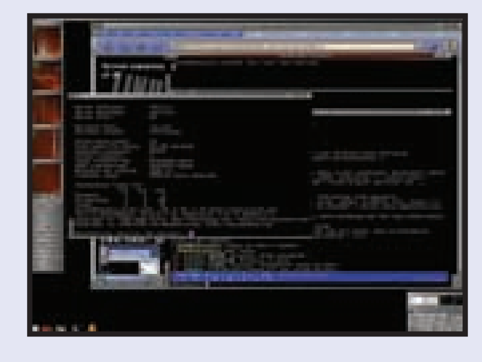


подходящими только под маску @*.*. Что же про другую сторону баррикад? В наличии атакующего - мозги + пылающее ненавистью сердце и жирный интернетовский канал. Здесь же попытаюсь обрисовать реальные способы социального инжиниринга, дабы не увеличивать размеры бан-листов различных каналов. При всем при этом подразумевается, что ты в курсе, о чем, собственно, идет речь. Не будем рассматривать захват далнетовских каналов, если ты не иркоп (а я на это надеюсь, ибо на данный момент россияне там не представлены), потому как это там хлопотное/неблагодарное занятие и куча ябед. Если на IRCнете твои хорошие знакомые - Tmh (irc.gate.ru) и серега (irc.msu.ru), можешь попробовать уговорить их покиллить весь вражеский канал и сделать тебя там опом (сомневаюсь, причем сильно, в успехе этого мероприятия).

Необходимый инструментарий

1. Знание команд IRC-серверов и клиентов различных приложений, умение писать скрипты "с ходу", т.е. не особо долго задумываясь, как это лучше сделать, уметь настраивать и устанавливать боты, уверенно управлять ботнетом.

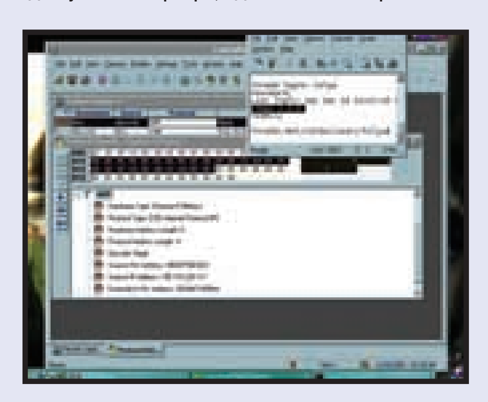
2. Нужно запастись как можно большим количеством free-шных шеллов, благо их полно. Но минус, что "халява" всегда перегружена пользователями и жутко тормозит, а имена хостов на халяве часто внушают подозрение. Яркий пример - *.pl, так уж получается, что с поляками и американцами у нас "теплые отношения", и могут забанить сразу или просто не пустить в канал, ибо на десятках каналов, где я побывал за последнее время, в IRCnet уже



стоял хронический бан на PL. Для справки, шелл - это, грубо говоря, телнетовский/ssh доступ на сервер с некоторыми возможностями (обычно IRC там входит в платные услуги, но есть даже такие, где можно откомпилировать и запустить собственного бота бесплатно). Найти можно, покопавшись в любой поисковой системе, а лучше во всех сразу, по запросу "freeshells" и откинув сообщения компаний, торгующих раковинами и машинными маслами :). Не в жилу маза? А я и не говорил, что все будет легко и непринужденно. Могут возникнуть осложнения при попытке зайти на иркнет со штатовских серваков - не резолвится DNS (посмотри www.arin.net) или просто данные сервера имеют k-line. Первая проблема решается просто, если имеется контакт на adm серванта шелл-провайдера: прописывается обратная зона для машины, т.е. присваивается свой vhost, который будет успешно резолвиться Lookin up ur host-name. Или же, когда руки админа кривы, как твои мозговые извилины :), можно отделаться установкой/активизацией identd (113-ый порт), куда частенько стучится Ircd, когда не может узнать доменное имя клиента.

Большинство открытых проксей (SOCKS`ов) не пускают на ирку, или наоборот, они закрыты на ирк-серваках K-лайнами. Советую переписать все слинкованные сервера заранее - список выдается в MIRCe командой /servers или /links, в BitchX не помню как ;), посмотри help.

3. Подключай всех знакомых, которые могут оказать посильную помощь - дать временный доступ на их сервера, сделать тебя на время бот-



мастером или владельцем их ботов (заставить перепрыгивать бота с канала на канал может только бот-мастер или их владелец - master/owner-статусы, соответственно).

Вот и все, можно приступать к захвату канала.

Let start a war...

Предполагается, что у мстительного товарища к этому моменту имеется приблизительно 6 ботов, полностью контролируемых, или столько же клиентов ирки, лучше, если это все-таки будет BitchX, - warscripts там специально встроены в клиента для этой цели. Не советую использовать экзотику: всякие графические приблуды, CIRC, QIRC и так далее - уж лучше старый добрый mIRC.

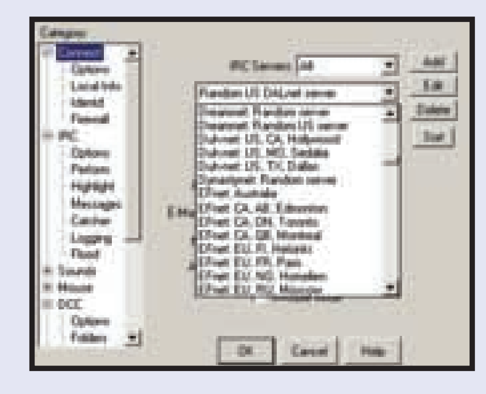
Итак:

1. Создаем стартовый канал, где можно поглядеть на свою банду, например, /j #REVENGE.

2. Притаскиваем туда все свои скудные запасы.

3. Настраиваем war-scripts, линкуем ботов, смотрим критические точки безопасности - выключаем опции kickflood, banflood, настраиваем ботов, чтобы на фингер молчали, версия - MIRC5.9, настраиваем +revenge, прописываем всех лучшими друзьями, для своего клиента мутим скрипт, который никого не кикает и не банит, а только выдает лучшим друзьям - опов пачками.

4. Заходим в чан жертвы, оставив ботов отдыхать на вновь созданном канале, пишем логи, смотрим, как там обстоят дела с безопасностью. Интересные моменты - кто есть кто на канале, желательно узнать, кто владелец, сколько мастеров, кто боты, кто операторы канала, могут

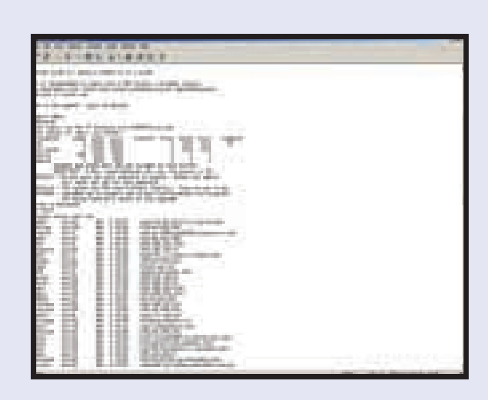


ли операторы раздавать опов, кто использует какие скрипты. Версии смотрим, используя /ver #Channel, где channel - название канала, дабы избежать выставленной опции kick_on_version - пусть попробуют кикнуть канал! :) Потом делаем /ping #channel и смотрим эхо. Маловероятно, но если у всех обитателей отклик меньше секунды - плохо дело.

5. Для захвата лучше выбрать день, когда постоянно идут сплиты. Сначала посмотреть - кто в сплите "улетает" из операторов и мастеров. Может статься так, что не придется просить одного-единственного опа - его подарит сам irc-сервер.

6. Доброжелательность на канале располагает обитателей подарить опа. Лучше - представиться





безобидной девушкой, болтать ни о чем, флиртовать, раздавать виртуальные поцелуи и фотографии со смазливой мордашкой. При этом кокетка на фото обнимает красивого плюшевого медвежонка - заметно понижает бдительность операторов (думаю, с этим не возникнет проблем - вклеишь медведя в фотошопе :). Получив случайно опа - не спеши сразу захватывать канал и рушить все одним махом, всели уверенность полной безобидности. Например, если все сидят из одной сетки/на одном irc-серваке, то может получиться, что в один прекрасный момент все упадут и останется только один оператор канала - тут можно сразу сделать +i на канал и заводить всю твою банду (маловероятно).

7. Время икс (определено заранее): получаем опа - приглашаем банду, дав сигнал (настроен скрипт), - например .massjoin #channel.

8. Банда врывается на канал, следует раздача участникам опов (ONJOIN: if ($nick AND $host inlist()) {addsendop()}), они начинают вырезать все что пытается оказать сопротивление - .mass-deop, .masskick, .massban.

9. Тут же канал закрывается на приватное использование, дабы не ворвались владельцы со своими друзьями или вернулись из сплита в немереном количестве. Наслаждаетесь феерическим зрелищем расправы над обитателями. Все, сказке конец.

Противопоказания

В заключение, хотелось бы сказать следующее: специально не привожу "рабочих скриптов", думаю, что народ грамотный, разберется со всем сам, оценит, стоит ли этим заниматься, так что это не более чем терминальное чтиво, дающее повод для размышлений. Мне, например, это уже просто неинтересно, отыгрался вдоволь прежде. Вероятность захвата канала способом, описанным выше, на какое-то время - максимальна, но можно и потерпеть фиаско. Не советую пытаться захватить #muppet_island - там уж больно много "крутых" владельцев - последний раз было около 67, не считая мастеров и опов. Так что при попытке атаки тебя встретит тотальный облом - вечный бан на многих каналах IRCNet-а. Попробуй познакомиться с настоящим бот-мастером - shura (www.shura.de). Его "шкурку" можно увидеть висящей на #СССР, #САРАТОВ. Трудно даже назвать количество ботов, подвластных этому хорошему человеку. В следующий раз попробую написать про варианты с использованием sniffеров и spoofеров, "подглядывание" паролей в IRC, алгоритм работы интеллектуальной болталки ELISA.

Халявный трафик в домашних сетях

Nikitos aka Surgeon (nikitos@atom.ru)

Ну чего, диалапщик, надоели тебе бесконечные дозвонки, дисконнекты, родственники, вечно висящие на телефоне, и МГТС с повременкой? Простым решением проблемы оказалось подключение к сетке с выходом в iNet. Сетке непростой, локальной да домашней, чтоб поблизости от жилища твоего была. Все тут хорошо, только уж больно трафик дорогой... Стоп.

Ты еще не подключился? Бегом давай в конторку, плати бабки, подключайся. Чтобы по-быстрому разыскать локалу в Москве, пройдись на lan.net.ru, там покоится наиболее обширный каталог домашних сеток Москвы. В подключении (его оплате) вряд ли тебе удастся помочь, а вот с трафиком, точнее его оплатой (неоплатой ;), мы в этой статье разберемся.

Подмена, разводка и прочее кидалово

Ты ведь тырил когда-нибудь Инет? Да-да, троянами, шарами, багами в домашних веб-серверах ;). Есть подобный опыт! Тут значительно все проще, никаких вирей и даже с юзером контактировать не придется... Как это так? А вот так. Во многих (читай - почти всех) московских сетках идентификация юзера при входе в сеть происходит только по ip-адресу.

А где он, окаянный, указывается? Правильно, в настройках. Ну так давай настроим их не попростому, а нормально, как и положено кульТхацкеру. Что тебе мешает указать не свой, а соседский ip-адрес? По существу препятствий НЕТ. Но не торопись... не только ip идентифицирует тебя в сети - есть такая штука, как MAC-адрес, или, говоря иначе, серийник сетевой карты. Как только ты нагонишь большой трафик юзеру, тот, естественно, пойдет к админам жаловаться. Те глянут в логи, и что они там увидят напротив сессии в 1 гиг? Правильно, твой MAC. Далее - поиск в базе айпишника, хозяином которого является чел с таким-то маком, у тебя в квартире гаснет свет, линк на сетевухе и раздается стук в дверь... далее, думаю, все известно из голливудского сценария "Хакеры в законе". Но не все так плохо, ведь MAC, как всякий номер, просто создан для его же подмены!

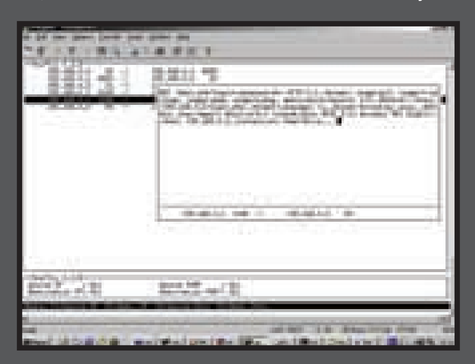
Но вот только менять на ЧТО? Да и КАК? Первая проблема решается весьма и весьма банально - запускаешь сниффер и любуешься на кучу активных МАКов/ИП, чужих паролей. Здесь же пролетит туча чужих писем, пароли на домашние странички, шеллы, конфигураторы роутеров... короче, все что носится по сети в незашифрованном (или слабокриптованном: dsniff+icq2k=luv) виде. Для танкистов, безвылазно сидящих в своем 43 года выпуска Т-34, следует, видимо, пояснить, что это такое... Но статья совершенно не про ЭТО, а посему держи линк: http://magazine1.xakep.ru/xa/021/044/1.asp. Там все толково и понятно расписано господином packet monkey, знатоком пакетов из-под чипсов - Дельтой.

Подборка боевого инвентаря

Выбор аппаратуры достаточно обширен: sniffit - http://reptile.rug.ac.be/~coder/sniffit/sniffit.html, неплохая рабочая лошадка; dsniff - http://www.monkey.org/~dugsong/dsniff/, добротный релиз, к которому можно прикрутить кучу плугинов.

После процедуры установки одного из sniffer`ов и запуска получаем список IP/MAC в сетке, прочитав несложный man по програм. Если ты имеешь дело с win-сетью, то иногда может помочь NB-сканер из Essential Net Tools. Тут ты увидишь MAC`и, ip, NB-имя и другую инфу :).

Итак, необходимая инфа захвачена, что делать дальше? Теперь жди глубокой ночи, когда эти упыри (соседи юзеры-вурдалаки) выключат компы, и айпишники освободятся. Понял к чему я?

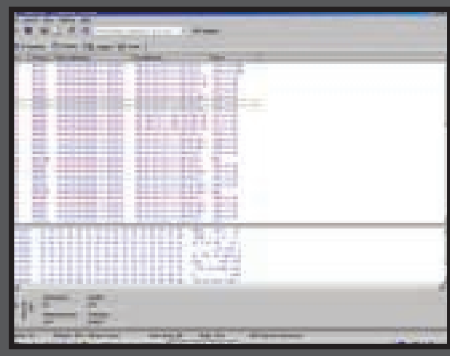


Правильно. Мы сейчас с тобой зайдем в сеть с чужим IP и не менее чужим MAC'ом и, естественно, работать будем за чужой счет :). Ну чего, воодушевился? Давай грузи пингвина (что ты так на меня смотришь-то? Я не говорил, что тут все просто...)

```
***
ifconfig ethX down
ifconfig ethX inet new-IP
ifconfig ethX hw ether new-MAC
ifconfig ethX up
Проверяем позаимствованные IP/MAC :
ifconfig ethX
***
```

GOT ROOT!

Молодца! Хочешь верь, хочешь не верь, но теперь ты сможешь абсолютно халявно лазить по Инету и качать мегатонные файлы! Только смотри не увлекайся работой с одного ip, а то, получив счета на тысячи баксов за трафик, твой злобо-сосед прийдет в гости с дробовиком и кувалдой :). Не хочется играть в Quake в домашних условиях? ОК, будь осторожней и финансовым беспределом не занимайся. Получается, что лучше нагреть 50 человек на 1 бакс, чем одного на полтос - враги не заметят, и тебе не скучно. Только не думай, что теперь ты неуловим - если ты сидишь глубокой ночью, то, вероятно, в этот момент в сети очень мало пользователей. Если сетка небольшая, то может так оказаться, что только ты и будешь сидеть...



Предположим, ты кинул чела на деньги. Он звонит к прову, говорит "Что ж это такое... Произвол! Средь бела дня деньги крадут...". Админ, посмотрев логи, устраивает "засаду" - ночью, когда ты с наивной лыбиной опять пойдешь варез качать, заспанный админ подойдет к хабу и с великой радостью увидит лампочку напротив твоего кабеля. Далее схема очевидна :(и напоминает обсужденный ранее киносценарий.

Ничем хорошим подобные разборки не светят, а поэтому давай там поосторожней... Не жадничай - "жадность хакера сгубила" ;). Поэтому можно наколбасить скрипт и скормить его дядюшке cron`y, который бы за тебя каждый час менял IP/MAC, выбирая данные из твоей database.

Противозачаточные

А как же быть, чтобы тебя сосед кул-хака не кинул на бабло, чтобы у тебя не крали трафик? Есть методы.

1. Психопатический метод. Купить UPS, поставить OpenBSD 2.9, настроить firewall и НИКОГДА не выключать комп.
2. Менее психопатический метод. Вести расписание, когда у тебя включен комп и когда ты сидишь в Инете. Запрашивать КАЖДЫЙ день логи у прова. И если увидишь там что-то подозрительное, то

сразу начинать спамить inbox админа сетки. Этот способ, к сожалению, не всегда помогает... Проверено ;(. Так что лучше юзать первый, психопатический =).

Prox рулит! NIRVANA(r)

Ищем в локалке винды с WinGate или Eserv (сканируя порты, телнетясь к ним и отыскивая баннеры нужных прог). И тупо прописываем в настройках твоего броузера IP, где ты нашел одну из этих прог. Если версия дырявая (вряд ли) или мозгов у кого-то нет (встречается часто) настолько, что чел дал доступ в Инет через свой прокс для локальщиков, ты получишь и халявный Инет =). Часто в локалках юзверы оставляют шары неприкрытыми или прячут за стандартной комбинацией Login&Password. Естественно, мы получаем к их машинам доступ и уже тогда устанавливаем все добро: баунсеры, соксы, порт-редиректы, фтп сервера... Короче, лох оказывается серьезным гейтом в Инет. Идеально подходит, когда чел имеет внешний, инетный IP на своей машине.

Телнетчики

После возлияния пива с админом сети можно выпросить не только халявные 100 мегов трафа. Имеется более симпатичная маза, часто незаметная извне глазу нехакерскому. Можно одолжить шелл на одном из серваков прова. Вполне стандартная просьба, к которой adm`ы относятся как к утреннему "чай с молоком будешь" или вечернему "еще наливать"? При хорошем контакте ответы бывают исключительно положительные. С полученным telnet/ssh (второй предпочтительнее - враги сниффать не будут) доступом можно творить чудеса. Понятное дело, можно ботов развесить да BitchX`ов всяких, только это мало поможет делу халявника. Нам нужен серьезный способ прогона. Их есть у меня! Воспользовавшись lynx или ftp, начинаем скачивать все необходимое в огромном объеме: фильмы, альбомы mp3, порник, дистрибутивы Linux... Закачать - закачали, а дальше что? А дальше качаем к себе все добро по локалке. Займет 5 сек, т.к. все польется по LAN, с фактически соседней машины. А то, что прову потом с отцовским ISP расплачиваться за гигагбайты, - уже не твоя проблема: ума-разума наберутся, научатся выставлять квоты на дисковое пространство и трафик.

Хакнутые хакеры

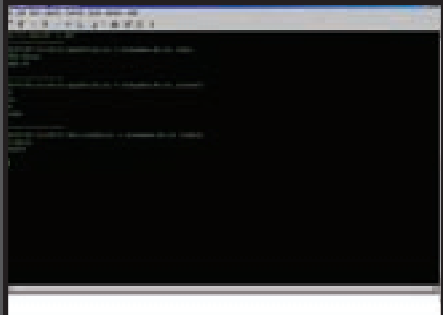
Ты поселился в большой сети? Тогда там есть прогрессивные ребята на линуксах и бздях. Замечательно! Через них тоже можно гонять трафик. Ведь далеко не все юниксойды хорошо в security разбираются, кто sendmail дырявый для эксперимента поставит, кто inetd конфигурнуть не сможет, где wu-ftp завис... Но к чему брата своего компьютерщика травить? Привнесем немного риска в его существование: будем прописывать чужие IP и MACи уже на его машину, да так, что когда обнаружится обман, - админы пойдут бить юниксойда ;), а не тебя. Главное - грамотно подмываться, т.е. вычищать логи.

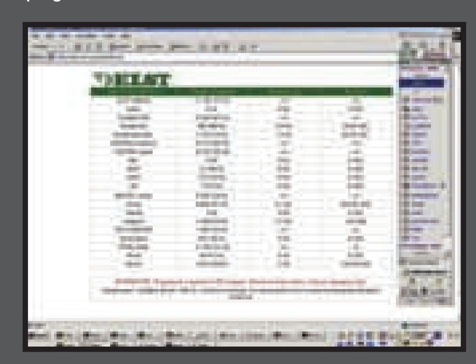
Зачистка

Если сеть не ахти какая большая, может появиться проблема: все пользователи на месте, у всех компы подключены в Сеть, все дружно работают,

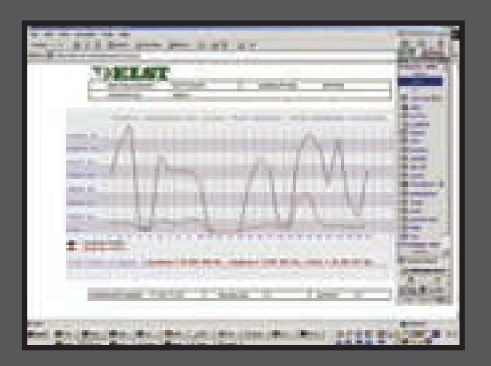


остается лишь парочка свободных ip/mac, которые и так опущены на десятки баксов. Что делать? Сетку, как село, захваченное "банд формированиями", во время антитеррористической операции, зачистить придется :). Т.е. вытряхнуть из сети ряд юзеров, дабы освободить адреса для собственного пользования.
Качаем jolt2.c (packetstormsecurity.org), компилим, запускаем:
./jolt2 -s <source IP> <victim IP>
В другом окне или ttyX пингуем для проверки:
ping -v -c 4 <victim IP>





Видим, что чувак слетел. Пытаемся занять его адрес. И тут облом - ip принимается, а Mac занят другим устройством :(. Такое происходит, т.к. машина подвисла, но остается включенной. Практика показывает, что после 5-6 зависаний от пользования компом отказывается основная часть юзверов... Жестоко, конечно, но что делать: придется стать на минутку серийным сетевым



убийцей :). Джолт - лишь один из множества способов обвала вражеской win-системы. Не стоит забывать про все еще актуальных грандов - CON/con и IGMP. Первый особенно катит в локалках, т.к. тут часто встречаются шары, часто достаточно грамотно прописанные, расположенные на базе 98-ых. Последнее-то нам особенно актуально: даем запрос по шарам о файле con/con и получаем подвисание удаленной системы. Оно нам и надо. Если же сетка крупная, то можно отдельных индивидуумов, висящих в удаленных частях, сбросить обычным пингом, упакованным в увесистые пакеты. А про igmp... Старый добрый voidozer под Винды и pimp/kod.c под *nix. До сих пор на этом баге спотыкаются, как минимум, 5% машин с Виндой. Устраиваешь massNUKE и освобождаешь кучу адресов, что хватит тебе и целой толпе халявщиков.

Договор

Про человеческий фактор в области халявного трафика мы уже говорили. Повторимся и сейчас. Большинство более-менее крупных сетей составляют договор с основным провом, от которого лежит канал в локалу, так что за российский трафик домашняя сеть не платит! Отсюда мазы: свои сотрудники, естественно, данный вид трафика не оплачивают. Кто мешает устроиться на минимальную занятость в контору? На небольшую деньгу и небольшую помощь с твоей стороны - рассчитывать не сложно, как и не сложно получить. Так что ты заимеешь фришный серфинг по России. Естественно, ты сможешь не только ползать по российским сайтам и трепаться в RU`шных IRC-сетях, а при минимальном желании тебе станет доступен и весь Запад! Всего-то нужен российский прокси-сервер, через который можно было бы перекачивать инфу. Или (что лучше) заиметь шелл на быстром серванте в России. Тогда ты сначала закатывал бы варез туда с Запада, а потом уже скачивал себе, оставаясь в российском сегменте и не оплачивая трафик. Сказка!

telnet – враг твой, провайдер!

X-KoDeX (root@hack4joy.com)

На хак-зарядку становись!

Когда приходит вдохновение на взлом? Естественно, когда пиво заканчивается, а водку организм принимает за страшнейший яд, но все равно истребляет без следа... Вот тогда, во времена тяжкие, организму открываются сотни консолей, стартуют компиляторы, посещаемость багтреков увеличивается вдвое. Тогда и я принялся за дело. Да и настроение в тот вечер было не очень, и я, плюнув на все (кроме подруги, естественно, та как раз закончила 3-ю симфонию на трубе :), пошел домой, в Сеть. На Ирке, как всегда, был дурдом, помоему даже боты были далеко не трезвы :). Почитав ньюсы, ответив на мыла, полазив по форумам, понял, что "делать что-то надо". Человек сам себе хозяин, и в каком он настроении (ну и состоянии, естественно ;), зависит только от самого человека. А скучать мне не по кайфу, вот и понеслось...

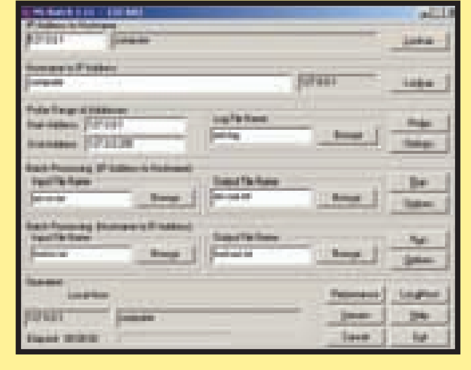
Карточная система

Меня давно интересовала относительно новая система "Internet по карточкам", и серванты авторизации еще не были опробованы мною на вкус. Решил я эту брешь закрыть посредством проверки на вшивость одного из таких провов.

Взял IP одного кекса из аськи, так как он недавно жаловался, что карточки подорожали, денег не хватает, и нес другую суицидальную чушь. Потом зашел на http://www.ripe.net/whois, узнал весь диапазон адресов.

Пров был небольшой, имел всего лишь один range IP-адресов класса С и пул на 160 модедиков (но это я узнал чуть позже). Дальше в ход был пущен NsBatch (DNS-сканнер такой), хотя можно было юзать и ShadowScan, там тоже есть такая фича, как "массовый" nslookup :). Вводишь диапазон адресов, и сканнер вытягивает с DNS-сервера имена этих самых хостов. После выдачи

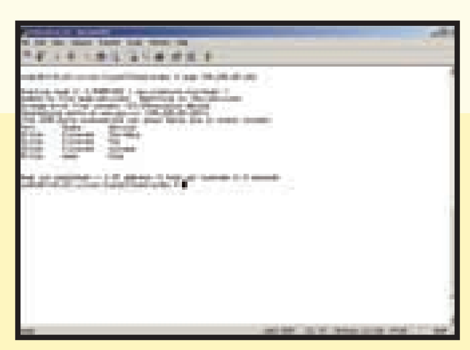




имен пришло какое-то "нейтральное" чувство, так как вся система прова была настроена довольно стандартно:

NS1	-	**212.*.*.1**
NS2	-	**212.*.*.2**
Default Gateway	-	**212.*.*.3**
POP/SMTP/NEWS	-	**212.*.*.4**
WWW/Shells/Proxy	-	**212.*.*.5**

На первых 2-ух сервантах стояла ФриБздя 4.0 (FreeBSD), на остальных Шапка 6.2 (Red Hat). Везде был открыт 22 порт и портянки стандартных демонов. Маленькое примечание: на "пятом" серванте еще работал rsh (514 порт). И все.



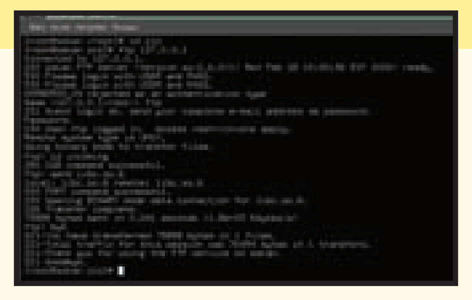
Проверку на дырявые cgi-скрипты решил оставить на потом, так как меня этот метод не особо пробивает. Остановил свое внимание на 212.*.*.5 . Открыты там были 21, 22, 23, 80, 3128 и 514 порты.

Telnetd/ftpd/spirtd и другие глупые демоны

Полез чесать, точнее чекать любимое место :). FTP-демон был версии wu-ftpd 2.6.0(1). Решил зайти туда, пров оказался добрым и предоставил стандартный набор прог и доков (вроде SPx, всяких upgrade'ов, патчей и т.д.) анонимному юзверю. Самое прекрасное было то, что присутствовал каталог incoming, зачем его админ поставил - было непонятно. И тут в голову ударила мысль! Вспомнил классическую атаку, основанную на ошибке в telnetd. И осуществил ее!

В чем заключается суть дыры?

Протокол телнета позволяет изменять в переменных окружения пути к библиотекам идентификации. А как "изменить", читай затроянить, LIBы проверки логина и пароля -][писал в одном из недавних номеров. В принципе, у каждого хакерюги должны быть "под рукой" такие библиотеки для различных ОС. Лучше потратить сутки на поиск, зато они всегда потом будут рядом.



Для Шапки 6.2 такая библиотека у меня уже была "заготовлена". Далее вся атака заняла не более 3 минут:

1. На ftp прова в каталог incoming была залита LIB'а libc.so.6, которая отвечает за аутентификацию на сервере.

```
[root@satan /root]# cd zlo
[root@satan zlo]# telnet
telnet> env define LD_LIBRARY_PATH /home/ftp/incoming
telnet> env export LD_LIBRARY_PATH
telnet> open 127.0.0.1
Trying 127.0.0.1...
Connected to satan (127.0.0.1).
Escape character is '^]'.

Red Hat Linux release 6.2 (Zoot)
Kernel 2.2.14-5.0smp on an i586
login: zlo
Password:
bash# cd /root
bash# 
```

2. Прописал пути в переменных окружения телнета путь к этой библиотеке и, собственно, прителнетился к серверу, ввел login/passwd, который до этого прописал в libc.so.6, и...

Усе :). Вот мы и "дома" :). Было найдено: оч-чень много аккаунтов по карточкам, но они меня как таковые не интересовали; подробная статистика по всем сеансам связи карточных юзарей и всякая прочая хрень, касающаяся обнаруженных аккаунтов - пров все-таки :).

На все про все ушло около 15 минут. Я стер логи своего пребывания, написал текст руту, засунул его в /root/zlo :) и набрал команду passwd, потом reboot, и все :). Допил похмельное пиво и со спокойной душой лег в люльку. Сутки прошли не даром...

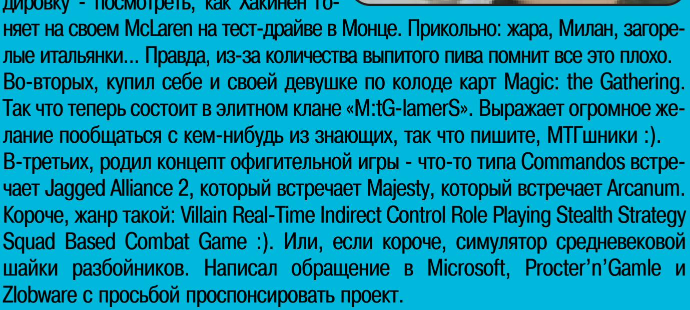
Хакер INSIDE

SINtez



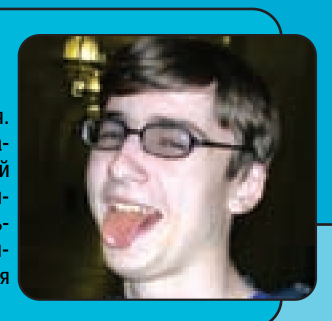
Совместно с Центнером осваивал новый (для нас) военный гамес - Operation Flashpoint. Параллельно качал различные шароварные проги, из которых особенно приколола новая версия NeoTrace. Дальнейшее время провел с любимым хобби - созданием видео-эффектов в Adobe Premiere и Adobe AfterFX. Из-за ночных сидений за компом поимел немереную бессонницу. Имел ее совместно с Сергеем Лукьяненко и его произведением «Геном», временами прерываясь на «Самоучитель Assembler», который моментально загонял в крепкий, беспробудный сон. Купил новую игрушку - Palm. Супер вещь! Два дня пытался научиться пользоваться его пером, в конке концов плюнул и решил юзать виртуальную клавиатуру. Но уже начинает подумывать о покупке хардверной клавы. Ну и, в конце концов, съездил вместе с Сайдом в Питер, на Chaos Construction. Отчет в этом же номере.

2poisonS



Во-первых, съездил в Италию, в командировку - посмотреть, как Хакинен гоняет на своем McLaren на тест-драйве в Монце. Прикольно: жара, Милан, загорелые итальянки... Правда, из-за количества выпитого пива помнит все это плохо. Во-вторых, купил себе и своей девушке по колоде карт Magic: the Gathering. Так что теперь состоит в элитном клане «M:tG-lamerS». Выражает огромное желание пообщаться с кем-нибудь из знающих, так что пишите, MTГшники :). В-третьих, родил концепт офигительной игры - что-то типа Commandos встречает Jagged Alliance 2, который встречает Majesty, который встречает Arcanum. Короче, жанр такой: Villain Real-Time Indirect Control Role Playing Stealth Strategy Squad Based Combat Game :). Или, если короче, симулятор средневековой шайки разбойников. Написал обращение в Microsoft, Procter'n'Gamle и Zlobware с просьбой проспонсировать проект.

CuTTer



Пришел к выводу, что экстремальный байк - его стихия. Гоняет на элитном BMX`е. Укатил к бабушке в Крым, дабы скрыться от редакторов, суливших урологический массаж за все хорошее. Пишет собственный IRC-баунсер на Си и бота на Перле. Пытается настроить кабель-модем 3Com под Linux. Совместно с Tonik[GiN] обучался поиску багов в Си-прогах. Ходил в поход, выражая ностальгию всего X-crew.

SideX

Покупал ежедневно квас в 5-литровую канистру, а также перешел с J7 на соки а-ля «совок» в стеклянных трехлитровках. Место Freebsd благополучно заняла новая культовая система NetBSD. После долгих бэкапов сбежал в Advanced Server Win XP из W2K server, чем это закончится - неизвестно... Решился прыгать с парашютом, но не был допущен по причине откормленности. Со спадом жары место водки и пива занял Absinth, ввезенный контрабандой на собственных плечах. Клубы, где от жары умирают кондишены, ушли в даун. Выбираемся на open-air`ы. Испытал культурно-физиологический шок во время посещения Doug&Martys Club: такого не было даже в Hungry duck...
С разболевшейся спиной узнал, что приятным бывает не только эротический массаж, но и лечебный. В кузове сервака поселились два P3-800 взамен прежнего, единственного P-667.

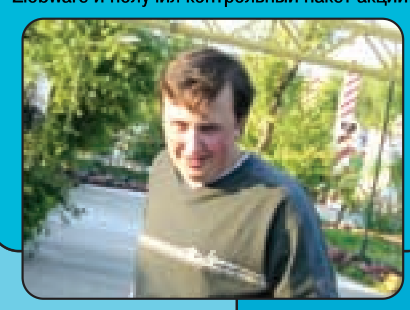
Hellman



Бурно отметил свой ДР в грузинском ресторане, получив презентом от X коллекционное трехлитровое пиво в рюкзаке с прилагаемыми кружками. Подсел на «кино без границ» в стиле Экстази/AcidHouse. Часто говорил о театре, но, по причине омертвления сезона, ограничивался лишь воспоминаниями о школьной роли Земляники в «Ревизоре». Хорошо отдохнул, получив одним из первых - приватный эксплойт на telnetd BSD-систем. Усталость ежедневных поездок на работу помогла в решении к переходу в статус remote admin`a. Снимал восходы солнца на цифровик. Готовит kernel security патчи для FreeBSD. Жди шока. Написал уникальную систему топов, порно-бароны отдыхают.

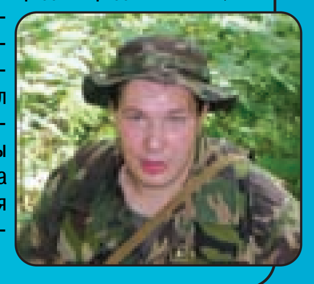
Delta

Поставил BlackBox, KDE сосет. Новые ощущения в отсутствие русской раскладки клавы. Официально изменил OpenBSD с Free, но при этом ведет половую жизнь и с NetBSD, которую по обряду древних друидов-юниксойдов можно ставить только ночью!
Гонял по встречной полосе на милицейской машине кента с мигалкой, совершил ДТП при гонках на картингах в ЦПКиО во время «Интервенции». Как и SideX, не был допущен к прыжкам с парашютом, по тем же reason`ам. Искал инвестора для запуска проекта ЗлобоДрома: открытого пространства для гонок на выживание на запорожцах. По неофициальным данным, стал президентом Zlobware и получил контрольный пакет акций.

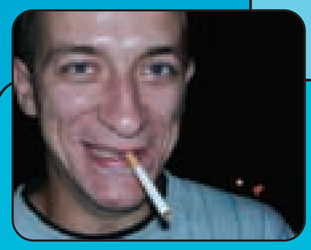


Centner

Занимался молодецким сексом с домашним компьютером, окончившимся полной победой и установкой целых трех операционок в его кремниевое чрево. Совершил несколько вылазок в леса, с целью поиска останков фашисткой Германии. Останки были найдены и учтены. Все медальоны российских воинов переданы родственникам, с указанием места гибели. В продолжение военных похождений организовал «Большие пейнтбольные маневры - Зона Хакера», на которых собирается занять пост генералиссимуса.



X-KoDeX



Перебрался в Москву. Активно потреблял сушеных кальмаров. Взломал банк спермы :). Научил телефонную линию слушаться модема. Пишет сканер а la nmap для распределенных сетей на Си. Питался окрошкой в «Дровах». После 5-летнего перерыва пошел в кино. Показывали «Кокаин». Окончив тестинг ряда московских duty-free диФчонок, дал обет безбрачия и целомудрия.

Учим Си: работа с указателями

Денис Мысенко (denis@mysenko.com)

Так, народ. Хватит халявничать, юзать чужие скрипты и эксплоиты, начинаем кодить сами. Если тебе кажется, что владеть языком – означает доставлять подруге удовольствие, то ты сильно ошибаешься, речь пойдет о вещи гораздо более сложной и сухой. Ты предпочитаешь Visual Basic? Удаляй как можно быстрее! Давно известно, что хакерский язык программирования – Си. Да, конечно, Дельфи тоже неплох, особенно для начинающих. И мы не зря описываем именно его в рубрике Кодинг.



Но после того (а лучше во время), как ты научишься кодить на Дельфях, тебе обязательно нужно изучить Си. Особенно это касается тех, кто хочет предложить свою руку и голову Линуксу, т.к. все экплойты под *nix пишутся именно на Си.

Для озабоченных историей: язык Си выдуман в конторе Bell Labs в США, а сам компилятор (сборщик запускных файлов из сорцов; сорцы (sources) - исходники) Си написан, соответственно, на языке Си (то есть на самом себе), что делает его особенно компактным и переносимым. Итак, приступим к описанию языка.

Типы данных

Под типами подразумеваются не братки, а виды какой-либо инфы, которую мы крутим в руках в процессе выполнения программы. Это могут быть цифры, буквы, слова (в том числе и матерные). Объявляются переменные в начале (в самом-самом начале) какой-нибудь из функций и юзаются, соответственно, в ней. Выглядит это так:

```
int ciferka, eshe_ciferka, i_eshe_ciferka;
char bukovka, eshe_bukovka, gy_gy;
char[20] materki;
```

Первое слово говорит о типе инфы, которая будет содержаться в переменной, затем идет перечисление (через запятую) имен, сколько переменных - столько и имен. Имя можешь делать какое угодно, лишь бы не с цифры начиналось и без всяких там минусов, т.е. юзай только английские буквы, цифры и знаки подчеркивания!

Типы могут быть следующие:

int - циферка
long int - боооольшая циферка
unsigned int - циферка, всегда положительная
void - пустышка, просто ничего
float - циферка с запятой
double - боооольшая циферка с запятой
char - символ, один символ!
char[X] - слово из X символов

Это, конечно, не все, но тебе для начала хватит :). Когда ты объявляешь все эти фишки, твоя программа, запустившись, будет под каждую забивать место в памяти, а если какая-то переменная останется неюзанной - компилятор при сборке начнет плакать.

Структура программы

Анатомия у программы на Си простая - это просто куча органов, то есть функций - мелких подпрограмм, никаких процедур и прочих аналов как таковых нет. Половым органом служит функция main, и если твой половой орган можно назвать тридцатью тремя грубыми и не очень словами, то в Си - это всегда main. С этой подпроги начинается запуск основной программы и только с нее, а что там дальше будет - дело твое. Кстати, function`ы возвращают какие-то значения, то есть после завершения они отдают какую-либо инфу функции, которая ее вызвала. Т.е. подпрограммку можно рассматривать как переменную, которая как-то хитро рассчитывается. Таким образом, получаем следующий скелет:

```
void main ()
{
 int blabla;
 char zlo;
 blabla = 5;
 zlo = 'A';
 blabla = zluka(3);
}
int zluka (int gygy)
{
 return (gygy + 2);
}
```

Итак, у нас определены две процедуры, главная и побочная. Первое слово в записи передает - какой тип инфы функция возвращает по завершении, если void - значит ничего не возвращает. Затем идет имя function`a, требова-

ния такие же, как и к имени переменной. Дальше в скобках перечисляются переменные и типы, которые функция берет от той, что ее вызывает. Называть их можешь, как хочешь, они чисто для внутреннего использования, а вот типы должны совпадать и даже в том же порядке. Не забывай! Если в скобках ничего не стоит, значит функции пофиг на погоду. Так, после объявления этих самых переменных идет открывающая фигурная скобка, в конце функции - закрывающая (никогда не забывай их ставить!), все что между - называют телом программы (ох, люблю тело - свое и женское :). Как видишь, в main у нас идет присвоение всяких там значений переменным. При присвоении всегда помни, что маза слева должна быть того же типа, что маза справа. Символы не забывай брать в амперстанды, цифры можешь писать как есть. В процедуре gygy использована команда return, она, типа, возвращает какую-то инфу той функции, которая ее вызвала, то есть - main. Синтаксис, как стало заметно, простой.

Указатели и стрелочники

Важной фишкой в кодинге на Си являются указатели, некие стрелочники, которые сами ничего юзабельного не содержат, а просто показывают пальцами на другие переменные. Типа есть у нас переменная int kaka, которая содержит цифру, так вот, int *byaka - указатель на какую-то циферку, снежинка говорит о том, что это указатель, byaka не содержит в себе ничего, она указывает на какую-нибудь переменную. Если в теле программы написать byaka = &kaka, то потом использование бяки будет равносильно использованию каки. Знак & перед именем в присвоении значит выдачу адреса переменной в памяти (только не говори, что ты не знал, что у любой переменной или не переменной есть свой адрес :), а указатель по своей ушлой натуре содержит в себе именно адрес. Сей adr и подлежит наводке стрелочников: стрелы переводить надо сюда.

Итак:

```
void main ()
{
 int kaka;
 int buka;
 int *byaka;

 kaka = 5;
 byaka = &kaka;
 buka = *byaka;
 printf("kaka = %d, byaka = %d, buka = %d
\n",
  kaka, *byaka, buka);
}
```

Во, какая сложная программулина. В начале объявляются цифры "кака" и "бука", а также указатель на какую-нибудь циферку "бяка". Затем кака становится равной 5, а бяка начинает метать стрелы на каку если чего, буке присваивается значение бяки, то есть каки (ведь бяка ссылается на каку сразу, а чтобы получить значение от указателя - надо поставить перед ним *, иначе это будет просто адрес памяти). Потом всемирно известный оператор printf() выводит все на штуку, называемую нынче монитором. Кстати, об использовании printf():

```
printf ("%d, %d, %c, какой-то текст\n",
kaka, buka, bukovka);
```

Оператор занимается выводом текста и переменных на экран, сначала в скобках идет текст, взятый в кавычки. Внутри текста, чтобы заюзать переменную, расставляем где надо специальные мазы - %d, %c, которые говорят о том, что их надо заменить переменными, которые пойдут дальше через запятую (соблюдай порядок, случайных связей берегись!). %d - значит циферка, %c - буковка, %s - слово или фраза, другие тебе пока не нужны. После любой запятой можно сделать перенос на следующую строку, не опасаясь за жизнь бук и бяк. Ах да, \n среди текста - значит перевод строки, \r - перевод каретки, \t - табуляция, \\ - чтобы получить сам символ \. Вообще же, если перед символом стоит \ - значит, символ не простой, а специальный. Есть еще операторы fprintf(), sprintf() - там все аналогично, только вывод идет соответственно в файл или в переменную типа строка, первым параметром в скобках задается имя переменной.

Заключение

Таким образом, ты теперь не полный балбес в Си, а что-то даже умеешь и понимаешь. В следующий раз я расскажу, как организована память (врага надо знать в лицо) и чего же с ней делать. Поверь, память играет такую же роль в хакинге, как петтинг в разводе девчонок.



Тест на хакерность

By Anal-[GiN]

Дискламер

Оговорюсь заранее, что в тесты, гороскопы, психологические тестирования, предсказания Павла Глобы и прочий бредогон – я не верю. И данный тест был нагло украден из одного модного женского журнала с небольшой заменой контекста вопроса и снабжением комментариями – противным, опасным для социума и психологически стабильных людей русским хацкерским языком :). Попадаются достаточно сложные вопросы, на которые в трезвом виде не смогли бы ответить и составители теста. Так что обрабатывая подобную шнягу, не стесняйся прибегать к дополнительным источникам информации. Как было у Рамблера: Эрудиция – не дар, а умение оперировать информацией. Большинство вопросов чисто технические, есть пара общих. Логика ответов практически одна и та же, так что во многих местах можно свободно ответить, не зная и сути проблемы :). Ценность правильных ответов разнится, где-то это 1, 2, 3 и даже 4. В некоторых вопросах два ответа являются правильными одновременно.

1.
Стандарт Golay используется:

1. В операционной системе BeOS
2. В системных блоках компьютеров Hewlett Packard
3. В системах пейджинговой связи
4. При написании скриптов TCL

2.
Что такое TCL?

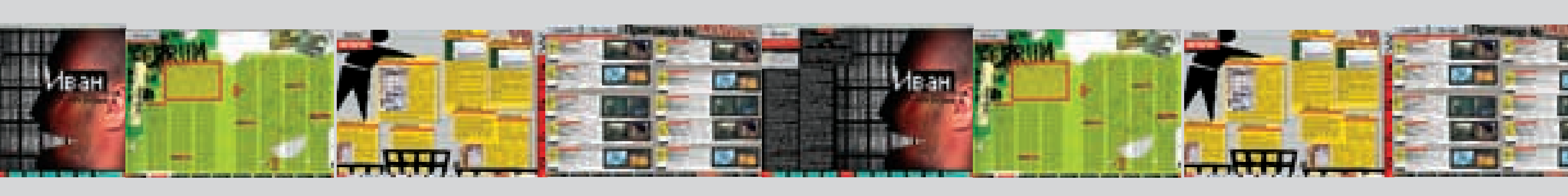
1. Это группа такая, где афро-американки поют реп
2. Technical Calling library в SunOS
3. Альбом Coldcut
4. "Язык программирования"

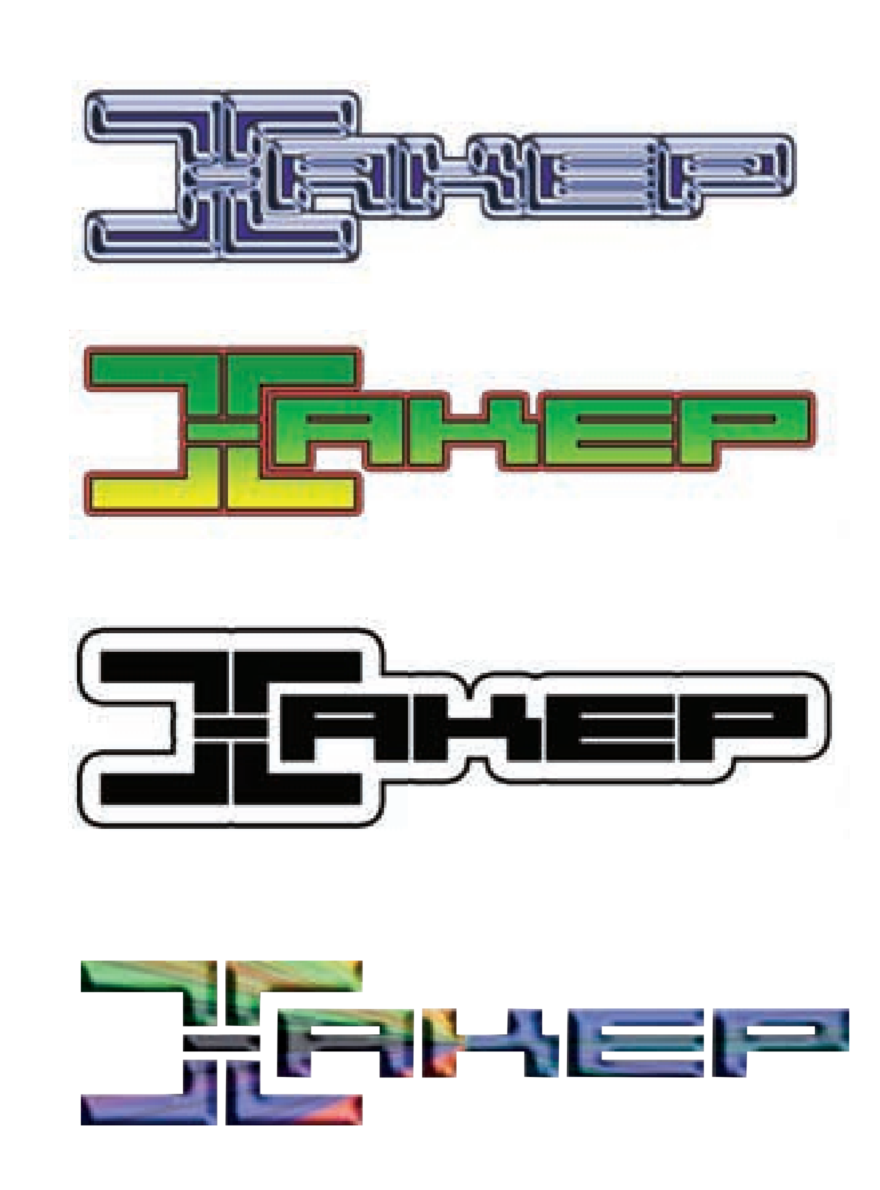
3.
Сколько максимально устройств поддерживает шина USB?

1. 31
2. 127
3. 2
4. Это же модель новых подгузников! Там устройство одно и то постоянно грязное.

4.
На чем строятся атаки формат строки?

1. Формат С:\


Иван


Хакер
Хакер
Хакер
Хакер

2. Строка с форматом %n
3. Переполнение форматированной строки
4. Неявно указанный формат

5.
Как обозначается новая строка в Perl`e:

1. \new
2. \n
3. \nl
4. \naher eto pisat`

6.
Я живу в 5020, означает:

1. Я живу в России
2. Я живу в Москве
3. Это hex-версия номера моей квартиры
4. Сам ты живешь тама, а я из Урюпинска

7.
На 143 порту, по RFC, висит:

1. Сервер трояна NetBus, в установках default
2. Злой негр Инет халявный раздает
3. Программа IMAIL версии 0.143
4. Сервис IMAP

8.
SUSIE является:

1. Сам соси
2. DNS-сервером в зоне SU
3. Дистрибутивом Linux
4. Хакерской командой, написавшей эксплойт на ftpd

9.
Kane Security используется для:

1. Получения прав root в *nix
2. Анализа защищенности сервера под управлением NT или целого домена
3. Выдачи 4-х новых видов оружия для бойца Kano из Mortal Combat
4. Обеспечения взлома "кодировки личного ключа DES"

10.
X.25 это:

1. Ускоритель Интернета, позволяющий увеличивать скорость соединения вплоть до 25 раз!
2. Продолжение протокола X3
3. Протокол, на котором построен ряд глобальных сетей, вроде Sprint, Роснет
4. Интернет по скриптам

11.
Какая из учетных записей относится к дефолтовым в WinNT?

1. root
2. guest
3. nobody
4. amgorb

12.
Kill PID несет в себе следующий смысл:

1. Ник хЭкера
2. Команда *nix, останавливающая процесс
3. Секретный код Q3 для консоли, убивающий всех вокруг
4. Серийный маньяк-гомосексуалист

13.
Приведите примеры баз данных:

1) FastDB
2) db3
3) Inetdb
4) Multidb

14.
Что не является дистрибутивом BSD-семейства?

1. BSDi
2. fsBSD
3. OpenBSD
4. NetBSD

15.
Главным образом я получаю почту от:

1. bugtraq`a, системы рассылок для кодеров, новостей IT/HiGH-tech, etc.
2. Девочек с веб-чата, служб знакомств, анекдоты, обзоры ВЕБа
3. Порно-серверов о новых бесплатных картинках
4. От издательства "Экстра-М" газету рекламную, там ТВ-программа на халяву!

16.
Teso – это:

1. Хакерская группа, поднявшаяся на эксплойтинге
2. Стиральный порошок
3. Футбольная команда из Никарагуа
4. Команда, которой можно менять пароли в OS Zlobatrix, аналог passwd

17.
Что означает поле TOS в ip заголовке версии 4?

1. Type Of Structure. Тип структуры посылаемого ip-пакета (запрос на соединение, запрос на разрыв связи, нормальный пакет)
2. Time Of Source. Тип места назначения (близко, далеко, очень далеко, другая вселенная)
3. Type Of Service. Тип сервиса (минимальная задержка, максимальная пропускная способность, максимальная надежность и минимальная стоимость)
4. Ничего не означает, все это бредни нетрезвого автора

Ответы:

1/3 - 3б
2/4 - 2б
3/2 - 2б
4/4 - 3б
5/2 - 2б
6/2 - 2б
7/4 - 1б
8/3 - 1б
9/2 - 3б
10/3 -2б
11/2 - 2б
12/2 - 2б
13/1 или 2 - 3б
14/2 - 2б
15/1-3б/2-1б/3-0б/4 - минус 1б
16/1 - 3б
17/3 - 4б

Калькуляция:

От 0 до 10
Надежда умирает последней
Твоей любимой программой должен стать man в юниксе, в виндах файлы readme.txt и ярлычок Help, все постинги в конфах закончатся знаком вопроса. Крайне тяжелый случай, который представляет интерес, т.к. позволяет заполнить пустоту головного полушария массой полезных знаний: токарное ремесло, профессия дояра, берегового боцмана, дегустатора мягких сыров и менеджера распространителя лапши "Досирак". На самом деле, скорее всего ты просто впервые читаешь журнал Х или позавчера выписался из психиатрически-реанимационного отделения больницы имени Склифосовского. При таком раскладе - главное не стесняться задавать вопросы, т.к. тогда есть шанс получить чисто хакерскую карточку психически клинического больного.

От 10 до 19
Haqer-d00d
С программой man ты уже познакомился, ярлык help был убран с рабочего стола, а половина устанавливаемых прог не удостаивается прочтения "ридми". Это подъем. Ты, очевидно, неплохо разбираешься в Windows и через полгода сможешь одеть на мускулистую грудь значок Wind0z-g00r00. Главное - не забывать о своем прогрессе: пользоваться не только готовыми прогами - писать нечто свое, попробовать работать в *nix`ах, BeOS`e, больше заниматься получением капитальных знаний, которые были бы полезны для усвоения сиюминутных.

От 20 до 28
Happy hax0r
Меня могут обвинить в иллюзорности и излишнем оптимизме, но, составляя тест, я предполагал, что большинство постоянных читателей Х попадет \m/ \m/ именно в эту категорию. Почему? Судя по результату, у тебя есть капитальные знания кодинга, Осей, стандартов, технологий. Также владеешь оперативной, наиболее актуальной информацией. В курсе событий сцены, постоянно в контакте с нужными людьми, участвуешь в проектах, состоишь в некой community (Gibbons Power :). Основная проблема, которая тормозит твой подъем на следующую ступень результата теста, - время. Время, которое кислородно необходимо для усвоения всей получаемой инфы, работы, обучения и прочей байды. Плюс стоит нарастить свое умение в работе с инфой так, чтобы даже самый каверзный вопрос решался за секунды, с использованием Яндекса и Альтависты :).

От 29 до 39
Digital g0d
Тут должно было быть многообещающее No comment. Два варианта людей могли набрать столько очков. Первый - реальные эрудиты от IT. Второй - умеющие пользоваться поисковиками и FAQ-архивами, usenet`ами :). Оба типа вызывают критическую симпатию и всем своим существованием дают хороший пример интеллектуального роста. Стоит заметить, что имеющиеся знания - вовсе не финал роста. Просто это хороший фундамент для дальнейшего часто значительно более быстрого подъема познания security и технологии.

Новости троянологического толка

DEIL AKA ТВАРЬ (DEIL@REAL.XAKEP.RU)

Привет, брателло! Сейчас я тебе поведаю о важном стратегическом материале – расскажу о некоторых из новинок мира трояписания, которые ежедневно, как грибы после дождя, появляются на просторах Интернета. Садись и слушай внимательно.

phAse zero 1.0

phAse zero - бета версия очередного бэкдора с интересной особенностью: его серверная часть каждый раз меняет размер при вызове клиентом. Данное чудо программерской мысли имеет вполне стандартный набор функций, а именно: скрытый или видимый запуск прог на удаленной машине, все функции работы с файлами, включая просмотр и закачку на удаленный комп; есть возможность работать с системным реестром, способствующая дальнейшей оптимизации и удалению ненужных (по твоему компетентному мнению) частей; также существует возможность залочить сервак или совсем прибить, чтоб люди в черном не нашли :). Конечно, данная программа имеет не очень много функций, но, по словам авторов, в полной версии будут доступны такие фишки, как: клавиатурный шпион, проигрыватель Media-файлов, возможность написания и подключения плагинов, а также многое другое. Что ж, подождем чуток и посмотрим, выполнят авторы свое обещание или нет.

SubSeven DEFCON8 2.1

О появлении на свет представленного подзаголовком трояна объявила всему миру компания Internet Security Systems, сказав, что данный зверь уже поразил около 800 компьютеров в США. Объявила и заодно поставила трояну оценку "4" по пятибальной шкале опасности. По мнению Криса Роуленда, главы X-Force, исследовательской группы компании ISS, с распространением этого монстра под угрозу ставится безопасность всего Интернета. Так почему же американцы столь обеспокоены появлением DEFCON-трояна? Причина кроется в способах использования зловредного троя: троянщики юзают зараженные системы для тестирования новых методик и стратегий DoS атак. Суть смертоносных нападений состоит в том, что одновременно с кучи ранее взломанных компов ("зомби", зомбаков по-нашему :) на сайт-жертву направляется нехилый поток ложных запросов, блокируя доступ для нормальных посетителей. Известно, что этот монстр, в отличие от предыдущих версий, использует для работы порт 16959 (новость дня, просто :).

Goga

Одна известная российская компания, занимающаяся разработкой антивирусных программ, сообщила об обнаружении троянской программы Goga, использующей в качестве носителя - файлы в популярном формате RTF (rich text format), который до сих пор считался неуязвимым для вирусов. Goga использует известную брешь в системе безопасности текстаписателя Microsoft Word, которая позволяет злоумышленнику незаметно для владельца компьютера запустить вредоносные коды сразу же после открытия зараженного документа. Если на компе не установлен нужный патч, то, при чтении зараженного файла формата RTF, MS Word загрузит с удаленного сайта шаблон, содержащий вредоносный макрос. Он, в свою очередь, извлечет из двоичной части RTF-файла дополнительную утилиту (круто, правда? :), которая тырит логины и пассы. После нахождения пассвордов пишется специальный текстовый файл под их хранение. Далее Goga запускает процедуру, которая публикует полученный текстовый файл на сайте общедоступных гостевых книг :), откуда автор троянской программы периодически получает похищенную информацию. Так что пользуйся блокнотом и почаще заглядывай на различные сайты с гостевухами :).

PRIORITY

PRIORITY - новый бэкдор с удобным интерфейсом (но пока в бета-тестировании). Прога напоминает собой SK Silencer (который, по словам автора PRIORITY, представляет собой ни что иное, как одну из первых версий PRIORITY, упертую и исправленную SmithClan'ом). Сразу после запуска серверной части на машине жертвы создается файл C:\Windows\System\PServer.exe. По умолчанию юзается порт 16969 (все любят позицию 69? :). Данная программулина позволяет: вести чат с другими клиентами, подключенными к данному серверу (чтобы поведать друг другу о самых аппетитных местах на харде ламака :) и жертвой; выключать и перезагружать администрируемую машину, разрывать связь с Инетом, выгружать непонравившиеся проги на компе жертвы, тырить пароли от аси, запускать проги, издавать душераздирающие звуки, показывать картинки и многое другое. Но особо меня порадовала функция Ping Pong, которая показывает на экране прыгающий шарик :). В финальной версии автор обещает сделать FTP сервер для администрирования дисков протрояненного долбака, который сам это делать не умеет :). В общем, неплохой троян (да и сервер весит не очень много), но будем ждать финальную версию с работающим ФТП.

W32.Leave.B.Worm

Данное творение уже не совсем троян. Это интернет-червь с функциями бэкдора. В качестве пути распространения W32.Leave.B.Worm эксплуатирует мыло - в письме, пришедшем якобы от службы технической поддержки Microsoft и похожем на письма от MS по стилю, ламаку предлагается скачать очередное исправление к продуктам софтверного гиганта. При этом в письме сообщается, что заплатка предназначается для защиты от нового вируса, способного уничтожать документы, стирать с диска mp3 и видео, заражать исполняемые файлы и портить BIOS. Его (W32.Leave.B.Worm) функциональность базируется на особом скрипт-языке, который позволяет удаленному хосту управлять зараженным компьютером. Червь также способен загружать и активизировать множество плагинов, в результате чего он может самостоятельно обновляться из Инета. После запуска троян копируется в системный каталог мастдая под именем REGSV.EXE. В главном компоненте червя есть текстовая строка, которая является мастер-паролем (!) от SubSeven'a. Таким образом Leave может самостоятельно администрировать машины, зараженные этим троем и устанавливаться на них. Серверная часть червя-трояна позволяет делать следующее: загружать с web-сайтов и активировать другие EXE-файлы (плагины червя), сканировать IP-адреса по заданной маске, подключаться к IRC-серверам и выполнять IRC-команды, создавать, перемещать, удалять, выполнять файлы на зараженной машине, а также многое другое. Команды скрипта зашифрованы с применением 64-битного ключа. Когда червь прогружает скрипт, происходит расшифровка и исполнение заразы. Червь также содержит в своем коде скрипт "по умолчанию" (который также зашифрован).



Обнаруженный SCP записывается в системный каталог Windows под именем ACI3.DLL.

Отличительной особенностью этого троянского зверя является возможность проведения DoS-атак. От подобной шняги уже пострадали: www.hotmail.com, www.internet.com, www.netscape.com, www.lycos.com, www.aol.com, www.msn.com, www.goto.com, www.excite.com, www.yahoo.com, www.altavista.com.

KRASS

О рождении новой звезды провозгласила фирма Trend Micro. Свежий троянец KRASS является еще одним бэкдором. Основная часть трояна - программа с хитрым и очень редким именем “Explorer.EXE”. Под маской овцы скрывается серверная часть троянца. Она позволяет управлять компьютером-жертвой удаленно, используя для этого 456 порт на машине лоха. Вот его (трояна, не лоха, или лоха с трояном, как тебе будет угодно :) основные возможности: полный доступ к диску (запись/чтение файлов), уничтожение файлов/директорий, запуск приложений, загрузка файлов, отслеживание процессов, запущенных на компьютере-жертве, получение RAS-паролей (пароли удаленного доступа). Клиент данного бэкдора содержит также некоторые полезные функции, позволяющие использовать его автономно. К тому же, трой имеет опцию изменения заголовков любых окон, свойств или кнопок, скрытый “переключатель”, который позволяет отключить для клиента доступ к любому диску. Чтобы активизировать эту опцию, необходимо добавить переключатель /SECRET %) в командную строку, тогда программа покажет четыре опции: Disable RAS Password (закрыть доступ к RAS-паролям), Disable Disk Access (отключить доступ к диску), Disable File Deleting (отрубить удаление файлов), загрузку файлов (Download), Disable Button Clicking (запретить нажатие кнопок).

Count2K

Зараза распространяется по электронной почте от лица службы технической поддержки корпорации Microsoft (оригинально, не правда ли?). Трой идет в файле с названием Y2KCOUNT.EXE длиной 124885 байт, прикрепленным к некоторому почтовому мессаджу. Внутри файла сидит самораспаковывающийся архив, собравший в себе Project1.exe, file001.dat, file002.dat, file003.dat, file004.dat. При обращении к архиву на экране появляется сообщение “Password protection error or invalid CRC32!” и стартует файлик Project1.exe, который копирует каждый из четырех dat-файлов в каталог WINDOWS\SYSTEM под именами Proclib.exe, Proclib.dll, Proclib16.dll, ntsvsrv.dll, Nlhvld.dll. Затем в секцию [boot] файла SYSTEM.INI в строку ‘drivers=’ записывается имя “ntsvsrv.dll”, что обеспечивает запуск троя при следующей перезагрузке системы. В момент перезагрузки файл WSOCK32.DLL в каталоге WINDOWS\SYSTEM переименовывается в Nlhvld.dll, затем Proclib16.dll переписывается в WSOCK32.DLL. Эта операция позволяет “трояну” подрубаться к Internet-соединению и запускать файл proclib.exe при каждом сеансе работы с Инетом. Цель работы нового монстра - перехват имени пользователя и пароля с их дальнейшей пересылкой автору.

Noname

Недавно появился на свет троян, который с зараженного компьютера рассылал обыкновенный рекламный спам. Утилита представляет собой обычный скрипт, написанный на VBS, рассылаемый в качестве аттачмента к электронному письму. Ребята из FirstNetSecurity.com впервые заподозрили подставу после того как вполне мирная 45-летняя женщина, хорошо известная провайдеру, была обвинена сразу несколькими возмущенными пользователями в спаме. После того как ламо запускает аттач, трой активизируется и прописывает себя в систему, после чего, незаметно для пользователя, начинает рассылать письмо рекламного содержания всем юзерам, содержащимся в адресной книге ламака, подписываясь его именем. В результате многочисленные знакомые (жители почтовой книги) получают от зомби письма с рекламой различных товаров, услуг и ресурсов. Как предполагают специалисты, в ближайшее время должен появиться платный релиз этой программы. По идее, трой был сбацан с помощью известной проги под названием “Visual Basic Worm Generator”, имеющей дружественный оконным интерфейс. Заимев подобную сладость, можно легко мутить любые вирусы, в том числе, как оказалось, и трояны-спаммеры.

Delphi. Центр управления полетами кнопки “Пуск”

Horrific (smirnandr@mail.ru) www.x-c-r.com

Помню, как я первый раз увидел Windows95. Мне так понравилась кнопка “Пуск”, что я ее полюбил до глубины “Выключить компьютер”. Вскоре в нашем институте обновили парк машин и на них тоже поставили Win95. Мне так захотелось приколоться над бедными однокурсниками, что я решил написать прогу, которая подбрасывала кнопку “Пуск”.



Сказано - сделано, написал и запустил на всех машинах. С каждым взлетом кнопки “Пуск” ламеры испуганно взлетали вместе с нею. А через некоторое время я увидел подобный прикол в Инете.



Предыстория

А что еще сказать? Все и так ясно. Сейчас я повторю свой предыдущий подвиг и покажу тебе, как самому написать такую прогу. Так что усаживайся поудобнее, наша кнопка “Пуск” взлетает на высоту 100 пикселей. И в этом нам поможет наш любимый дядя Борман с великолепным другом Delphi.

Но, прежде чем начать, нужно подготовить картинку с изображением кнопки “Пуск”. Для этого ты можешь нарисовать ее своими руками в любом графическом редакторе. Ну а если ты IBM совместимый чел, то можешь нажать кнопку Print Screen, чтобы запомнить содержимое экрана и вставить его в любом графическом редакторе. Далее, простыми манипуляциями, вытягивай изображение кнопки в отдельный файл.

10-секундная готовность

Создавай новый проект в Delphi. Сразу сохрани его. Теперь измени параметры окна. Для этого лезь в объектный инспектор. Здесь устанавливай параметр BorderStyle в bsNone, чтобы у него не было никаких обрамлений. А параметр FormStyle устанавливай в fsStayOnTop, чтобы окно всегда располагалось поверх других. Все, форма готова. Теперь нужно бросить на форму компонент Image с палитры компонентов Additional. На форме появится соответствующий компонент с именем Image1. Щелкни по нему и снова переходи в объектный инспектор. Параметр Left и Top установи в 0, чтобы картинка располагалась точно в левом верхнем углу.

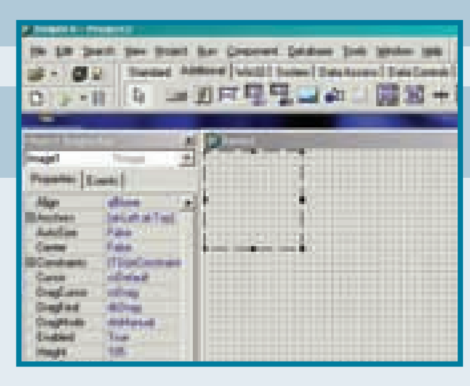
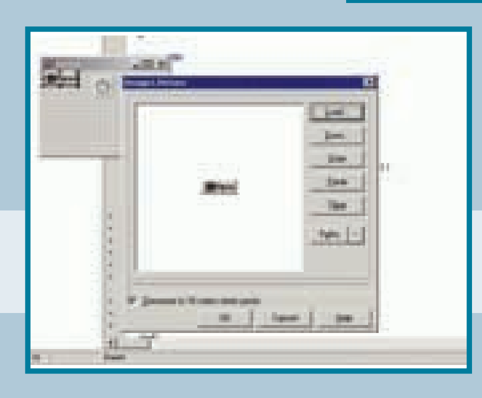


рисунок 1

Теперь дважды щелкни по параметру Picture, и перед тобой появится окно, в котором можно загрузить в компонент картинку (рисунок 1). Нажми кнопку “Load” и выбери файл, в котором у тебя сохранена картинка кнопки “Пуск”. После этого установи свойство AutoSize у Image1 в true, чтобы компонент стал размером с рисунок.

OK. Форма почти готова. Осталось только поправить ширину и высоту окна, чтобы оно было размером с картинку. С высотой у тебя проблем не будет. Ты можешь без проблем менять ее как угодно. А вот ширина не может быть меньше чем ширина кнопок на обрамлении. Но и это мы победим.



Листинг 1

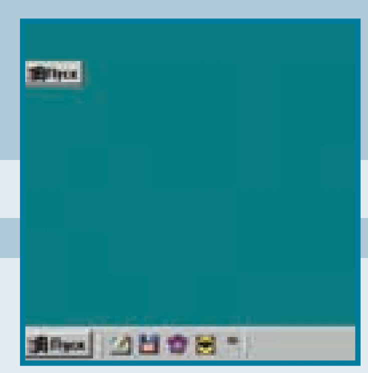
```
procedure TForm1.FormShow(Sender: TObject);
begin
 Width:=51;//Установить ширину окна
 Height:=21;//Установить высоту
 Left:=-100;//Убрать окно за левую границу экрана.
end;
```

Щелкни по форме и перейди на закладку Events. Дважды щелкни по событию OnShow, чтобы создать такой обработчик события. Он будет вызываться при показе окна. В нем напиши содержимое листинга 1. Здесь я устанавливаю значения ширины и высоты окна. Как ты помнишь, у нас были проблемы с установкой этих значений визуально, а так мы в наглую задаем то, что нам нужно.

Значения могут быть другими, все зависит от того, какого размера получилась кнопка. Моя вышла габаритами 21x51.

Центр Управления Полетами

Теперь брось на форму Timer с палитры компонентов System. В его свойствах нужно изменить значение Interval. По умолчанию оно равно 1000 миллисекундам (1 секунда). Для нас больше подойдет 10000 (10 секунд). Не резон, если "Пуск" будет



летать каждую секунду. Такими темпами он может даже не успеть приземлится. Теперь перейди на закладку Events и дважды щелкни по событию OnTimer. Создастся обработчик события, который будет вызываться каждые 10 секунд (значение свойства Interval). Здесь мы развернем центр управления полетом кнопки "Пуск". В этом обработчике напиши содержимое листинга 2. Я не буду описывать его содержимое, потому что журнал не резиновый. Так что смотри на комментарии, там можно со всем разобраться.

В принципе, прога готова, и ее можно запускать. Но если ты сделаешь это, то она засветится в TaskBar, что абсолютно недопустимо для проги-прикола. Давай напишем код, который спрячет наше приложение от грозного глаза Taskbar. Для этого выбери пункт меню View Source из меню Project. Перед тобой появится исходник самого проекта. Сравни его с листингом 3 и нужное допиши. Чтобы тебе было проще, изменения произошли там, где есть комментарии.

Листинг 2

```
procedure TForm1.Timer1Timer(Sender: TObject);
var
 i:Integer;
 h:THandle;
begin
//Сделать окно видимым.
 Visible:=true;
//Установить верхнюю позицию окна в левый
//нижний угол экрана.
 Top:=Screen.Height-Height;
 Left:=1;
//Создаю пустой указатель h, который буду
//использовать для задержки.
 h:=CreateEvent(nil, true,false, 'et');

//Сейчас будем подымать кнопку
// От 1 до 80 выполнять
//действия от begin до end
 for i:=1 to 80 do
  begin
  //Увеличить значение верхней
  //позиции окна с кнопкой.
   Top:=Screen.Height-Height-i*5;
   Repaint; //Перерисовать окно
   WaitForSingleObject(h,15);
//Задержка в 5 миллисекунд.
  end;

//Дальше идет опускание кнопки
//Алгоритм тот же, просто выполнение
//идет в обратном порядке
 for i:=80 downto 1 do
  begin
   Top:=Screen.Height-Height-i*5;
   Repaint;
   WaitForSingleObject(h,15);
  end;

//Уничтожаю указатель h
 Closehandle(h);
//Прячу окно.
 Visible:=false;
end;
```

Он сказал "поехали" и махнул рукой

Все. Играйся на здоровье. Только будь осторожен. Слабонервные ламеры при виде летающей кнопки могут уйти в бессознательное состояние на пару десятков лет. Нашатырь тут уже не поможет. Так что за побочные действия отвечать будешь сам.

Исходники примера ты можешь найти у меня на странице **www.x-c-r.com**.

Листинг 3

```
program Project1;
uses
  Forms,
  Windows,// Это я добавил модуль Windows
  Unit1 in 'Unit1.pas' {Form1};
{$R *.RES}
//Далее я добавил новую переменную
var EStyle : integer;
begin
  Application.Initialize;
//Далее идет установка невидимости приложения
  EStyle:=GetWindowLong(application.Handle, GWL_EXSTYLE);
  SetWindowLong(Application.Handle, GWL_EXSTYLE,
    EStyle or WS_EX_TOOLWINDOW);
//Остальное не менять
  Application.CreateForm(TForm1, Form1);
  Application.Run;
end.
```

Kylix. Работа с компонентами

(Внимание!!! Пример, написанный в Kylix, прекрасно работает в Delphi)

Horrific (smirnandr@mail.ru) www.x-c-r.com

Многие говорят, что в Linux нет хорошего файл менеджера типа Windows Commander под Windows. Это не так. Менеджеры есть, может они не совсем удобны и не на столько функциональны, но они есть. А если ты все же хочешь получить супер файл–менеджер, то все в твоих руках. Попробуй написать его сам. Для этого нужно не так уж и много сил, особенно с Kylix.

Предыстория

В этой статье я хочу тебе показать, как самому написать подобие файлового менеджера. Хотя он будет пустой, некрасивый и не очень функционален, но все же он будет. Нам главное - понять основы работы с файлами. Со временем ты сможешь улучшить и приукрасить свое творение. А я буду тебе помогать.

Итак. Даю установку. Наша задача написать прогу, с помощью которой можно будет прогуливаться по каталогам. Установка дана. Вперед!!!

На старт

Запускай Kylix, мы начинаем с чистого листа. Брось на форму два компонента: ListView с палитры компонентов Common Controls и ControlBar с палитры Additional. У тебя получится два компонента с именами ListView1 и ControlBar1. У ControlBar1 свойство Align нужно установить в alTop, а у ListView1 в alClient..

Теперь на ControlBar1 брось Combobox с палитры Standard. После этого у ControlBar1 измени свойство AutoSize в true. Все. Больше никаких компонентов нам не понадобится. Графический интерфейс нашего файлового менеджера пока готов. Надеюсь, что у тебя получилось нечто похожее на рисунок 1. Если получилось лучше, то это твои проблемы.

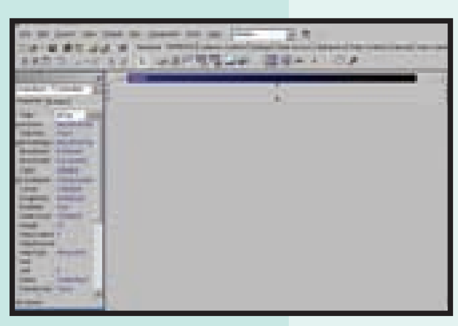


рисунок 1

Теперь нам нужно выловить событие OnShow (когда показывается форма) главной формы. По этому событию мы всегда будем производить инициализацию различных примочек. Итак, выдели форму. Как это сделать, если на нашей форме нет чистого места? Везде сплошные компоненты. Для этого вверху окна объектного инспектора есть выпадающий список. В этом списке перечислены все компоненты на форме. Найди в этом списке имя формы (по умолчанию это Form1, если ты не менял). Так ты сможешь выделить форму.

Листинг 1

```
procedure TForm1.ListView1DblClick(Sender: TObject);
begin
//Если ты дважды щелкнул по элементу “точка”, то path:=’/’
 if ListView1.Selected.Caption=’.’ then Path:=’/’
 else
//Если по двум точкам, то подняться на один уровень
  if ListView1.Selected.Caption=’..’ then
   begin
    path:=copy(Path,1,Length(Path)-1);
    Path:=ExtractFilePath(Path);
   end
  else
//Если не то и не другое, то, значит, ты щелкнул по папке.
//Значит, надо прибавить к текущему пути имя папки
   Path:=Path+ListView1.Selected.Caption+’/’;
//Перечитываем содержимое нового пути.
 ListDir(Path);
end;
```

Теперь перейди на закладку Events и создай обработчик для события OnShow. Там нужно написать содержимое листинга 1. Тут всего лишь один вызов процедуры ListDir. Эта процедура читает содержимое директории, указанной в качестве единственного параметра. Но такой процедуры в Kylix нет, я ее выдумал :), поэтому нам придется написать ее самим.

Найди раздел private в объявлении формы. Где искать, я писал пару номеров назад. Если ты пролетал в облаках, то просто ищи слово private и после него пиши следующее:

```
private
  { Private declarations }
  Path:String;
  procedure ListDir(dir:String);
```

Path - это переменная, в которой всегда будет храниться текущий путь на диске. ListDir - это наша процедура. Теперь нажми Ctrl+Alt+C, и Kylix сам создаст необходимую заготовку для новой процедуры. В нее напиши все что написано в листинге 2. Комментарии помогут тебе разобраться с происходящим, а я рассмотрю самые интересные моменты.

Во-первых, это очень интересная конструкция if ... then. Она читается как “Если Какое-то Условие верно, то выполнить действие”. Если после этого стоят begin и end, то выполняются все действия между ними, иначе только одно следующее действие. В нашем случае запускается поиск с помощью функции FindFirst. Если она вернула какое-то значение, то выполнится все, что идет после, между begin и end. Между begin и end выполняется цикл:

```
repeat
 Действие
until Условие;
```

Этот цикл последовательно выполняет “Действие”, пока “Условие” верно. В качестве условия у нас стоит функция, возвращающая следующий найденный файл. Пока файлы находятся сами собой, будет выполняться действие, которое заполняет ListView1 именами найденных файлов.

Листинг 2

```
procedure TForm1.ListDir(dir: String);
var
  sr: TSearchRec;
begin
//Очистить содержимое ListView1
 ListView1.Items.Clear;
 //Начать поиск и найти первый файл.
 if FindFirst(dir+'*', faAnyFile, sr) = 0 then
  begin
   repeat
// Добавить в ListView1 имя
//найденного файла
    ListView1.Items.Add.Caption:=sr.Name;
//Найти следующий файл и перейти
//на repeat.
  until FindNext(sr) <> 0;
//Закрыть поиск
    FindClose(sr);
   end;

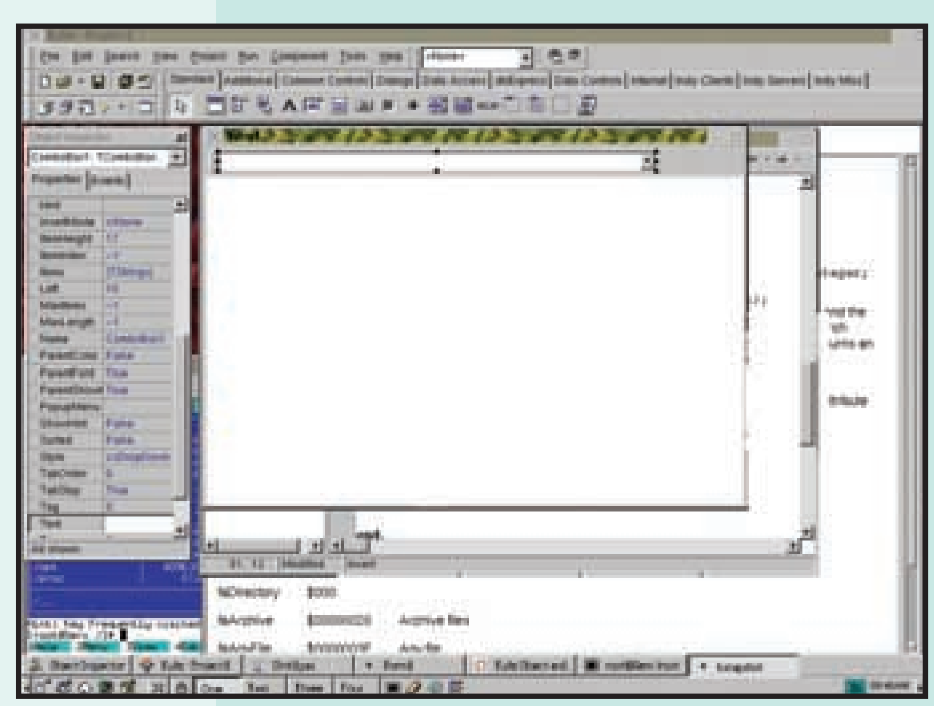
//Запомнить текущее положение пути
 Path:=dir;

//Если этого пути нет в выпадающем
//списке ComboBox1, то добавить его
 if ComboBox1.Items.IndexOf(Path)=-1 then
  ComboBox1.Items.Add(Path);

//Если количество элементов
//в ComboBox1 больше 20 то
//удалить первый
 if ComboBox1.Items.count>20 then
  ComboBox1.Items.Delete(0);

//Показать путь в строке ComboBox1.Text
 ComboBox1.Text:=Path;
end;
```

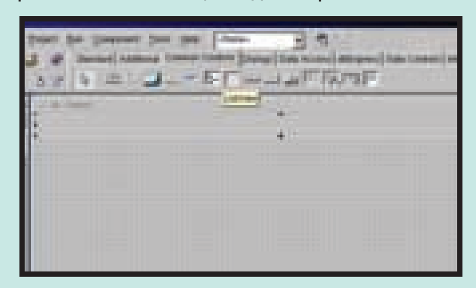
Все. Все остальное можно понять по комментариям. Так что теперь давай еще немного поШкодим. Для этого вернись к форме. Выдели компонент ListView1 и создай для него обработчик события OnDblClick. В этом обработчике напиши все, что есть в листинге 3.



Этим мы поймали событие двойного клика по элементу из ListView и перешли в новое место на диске.

Заключение

Конечно же, в проге еще полно недостатков, но она работает. Нам главное - понять принцип, а дальше уже полетим как на коньках. Для общего развития можешь еще создать обработчик события OnChange у ComboBox1 и написать туда одну лишь строку: ListDir(Combobox1.Text);. Так ты сможешь переходить в любую папку, сохраненную в Combobox1.



Листинг 3

```
procedure TForm1.FormShow(Sender:
TObject);
begin
 ListDir('/');
end;
```

Со временем мы будем улучшать пример, а улучшать есть что. Например, нужно по-разному отображать и обрабатывать файлы и папки. А в данном варианте, если ты дважды кликнешь по файлу, то прога будет пытаться его открыть как папку. Ну, в общем, работы еще полно. Так что встретимся через месяц на том же месте.

Примеры можно забрать на www.x-c-r.com



20 советов по созданию настоящего X-кода

Иван Скляров (sklyarovivan@mail.ru)

Хочешь, чтобы созданные тобой проги заслужили уважение, а не выкрики must die, и, чтобы, увидав код твоей программы, знающие люди говорили: “Это писал настоящий хакер!”. Тогда всегда следуй тем двадцати советам, что ты здесь прочитаешь, и не важно, на каком языке ты кодишь – они подходят для всех существующих языков программирования.

Советы эти, главным образом, посвящены оптимизации, т.е. созданию быстрого и потребляющего малое количество ресурсов (памяти, свободного места на винте и т.п.) кода, а потому и безглючного. В наше время, когда на первом месте стоит срок разработки программы, а не ее качество, оптимизация разработчикам стала не нужна. Поэтому и приходится бедным юзерам с очередным выходом форточек апгрейдить свою тачку, а также бороться с вечными глюками. Но остались еще люди - создатели Linux, Back Orifice 2000 и т.п., которым в первую очередь важны не деньги, а честь и уважение своего имени, - ты, наверное, понял, что я говорю о хакерах. Теперь и у тебя есть возможность делать как они.

Вообще, часть этих советов раньше можно было встретить в любой книге по языкам программирования для начинающих. Но современные авторы считают это лишним, наивно полагая, что современные компиляторы сами сделают все за программиста. Я согласен, что компиляторы стали более интеллектуальны, но надеяться на них я бы не советовал, тем более, есть еще и интерпретируемые языки, такие как Perl, которым оптимизация просто необходима, да и не нужно приучать новичков к дурному тону программирования.

Совет #1

Старайся писать небольшой и компактный код. Запомни: число строк и их длина прямо пропорциональны размеру скомпилированной программы. К тому же компактный код делает программы более шустрыми. У опытных программистов существует даже такая заповедь: “Нет такой программы, которую нельзя было бы уменьшить хотя бы на один оператор”. Поэтому всегда внимательно смотри листинг своей программы, и ты обязательно обнаружишь места, которые можно написать короче или вообще убрать. Но это не касается комментариев, компилятор их все равно игнорирует, поэтому всегда вставляй комментарии, особенно в больших и сложных программах. Это поможет тебе легче в них ориентироваться, к тому же, если ты вдруг решишь продать тексты своих программ, то комментарии повысят им цену.

Совет #2

Хорошенько изучи IDE (интегрированная среда разработчика) языка, на котором ты кодишь. Обычно в опциях IDE имеется возможность выбирать различные типы компиляторов, а по умолчанию всегда стоит самый простой, который быстро компилирует, но создает менее оптимизированный код. Поэтому всегда устанавливай самый оптимизирующий тип компилятора, и если ты не пишешь очередные форточки, то его медленная скорость будет для тебя не особо обременительна. В крайнем случае для черновых версий своих программ можешь использовать обычный тип компилятора, а для окончательного варианта - самый оптимизирующий. Кроме того, если имеется возможность, установи компилятор в режим “предупреждений о максимальном числе ситуаций” и исправляй свою программу до полного исчезновения сообщений.

Совет #3

Используй вставки на ассемблере. Конечно, можно посоветовать полностью писать программы на асме, но надо признать, что сделать сейчас что-то более-менее крупное на нем не так-то просто и быстро, но возможность применить в своей программе вставку на ассемблере никогда не упускай. Это значительно повысит производительность программы и уменьшит ее требовательность к ресурсам компьютера. Тем более, практически все языки высокого уровня позволяют делать это. Кстати, всемирно известный в компьютерном мире Стив Гибсон, специалист по компьютерной безопасности, всегда писал и до сих пор пишет свои программы исключительно на ассемблере. Учи ассемблер!

Совет #4

Не выделывайся - делай стандартный и простой интерфейс в своих прогах. Не нужно использовать модные сейчас окна нестандартной формы (овальные, треугольные и т.п.), необычные кнопки, оригинальные меню и т.п. Все это сильно тормозит программу, расходует огромное количество ресурсов компьютера и требует дополнительного времени на разработку. Тем более, профессионалов этим не удивишь, а простые юзеры тебя просто не поймут. Пользователю всегда удобней и легче использовать мерзкий виндовый интерфейс, чем разбираться в чем-то новом и необычном. Поэтому все твои труды могут просто пойти насмарку, да и если уж пишешь под какую-

нибудь ось - смирись с ее правилами и стандартами. Вообще, под необычным и пестрым интерфейсом, как правило, авторы стараются скрыть убогость и малую функциональность своих прог, подобные интерфейсы позволительны только гамесам и развлекухам. Посмотри на тот же BO2k - все просто и стандартно, а настоящий UNIX так это вообще обычный shell - строка для ввода команд.

Совет #5

Обязательно изучи размер в байтах всех типов переменных языка, на котором ты кодишь. И не используй "большие" типы переменных, когда этого не требуется, т.к. это ведет к лишнему расходу памяти, к тому же типы переменных, занимающие большее количество памяти, работают медленнее тех, которые требуют меньше памяти. Например, в VB есть такой тормозной тип переменной, как Variant, который занимает 16 байт, хотя в большинстве случаев вместо него можно использовать другие типы переменных, например Double, требующий всего 8 байт.

Совет #6

Всегда явно указывай типы всех используемых тобой переменных, даже если язык программирования позволяет этого не делать. Например, в VB тип переменной указывается так: Dim X As Integer. Но если этого не сделать, то по умолчанию переменной X будет присвоен тип Variant (16 байт) вместо необходимого Integer, требующего всего 2 байта памяти.

Совет #7

Помни, что глобальные переменные (extern), а также статические переменные (static) работают в несколько раз медленнее и требуют больше памяти, чем локальные и автоматические переменные (автоматические переменные сохраняют свое значение, пока выполняется процедура, и теряются при выходе из нее). Локальные и автоматические переменные, как правило, объявлены по умолчанию. Поэтому вместо объявления глобальных и статических переменных лучше использовать, например, переменные уровня модуля.

Совет #8

Старайся использовать простые арифметические операции типа сложения или вычитания, т.к. процессор выполняет их гораздо быстрее, чем, например, умножение или деление. Вообще, все арифметические операции можно разделить по скорости выполнения их процессором. Вот некоторые из них, начиная с самой быстрой:

1) присваивание;
2) сложение/вычитание;
3) умножение;
4) деление;
5) возведение в степень и др.

Для того чтобы перейти от сложных операций к более простым, сокращай выражения, например, вместо x = a*c + b*c + a*d + b*d правильнее написать x = (a + b)*(c + d). Деление заменяй умножением, например, вместо x = (a + b)/2 пиши x = (a + b)*0,5. Если тебе нужно возвести число в степень, лучше использовать произведение этого числа на само себя. Это будет гораздо быстрее, чем операция ^ в VB или функция pow(x, y) в C/C++. Например, выражение y = x * x * x будет выполнено в 7 раз быстрее, чем y = x ^ 3. Если степень высокого порядка, то ее лучше разбить с помощью временных переменных, например:

```
tmp = x * x * x
y = tmp * tmp * x
```

Это будет выполнено в 3 раза быстрее, чем x ^ 7.

Совет #9

Если позволяет твой язык программирования, используй сокращенные операции. Например, такие как в C/C++: инкремент ++ (увеличение на 1), декремент -- (уменьшение на 1), а также операции присваивания, типа += (выражение x += 3 то же самое, что x = x + 3) и т.п. Сокращенные операции выполняются быстрее, кроме того, они позволяют быстрее набивать программу, и компилятор быстрее ее компилирует.

Совет #10

Ты должен знать, что в программировании считается ламерством использовать оператор Goto. Давно доказано, что без него можно обойтись в любой ситуации. Использование этого оператора ухудшает читаемость программы и увеличивает код, правда, в некоторых ситуациях может повысить эффективность. Но даже если ты используешь его для повышения эффективности своей проги, все равно никому не показывай ее текст, т.к. любой опытный программер, увидев оператор Goto, сразу примет тебя за ламера.

Совет #11

Если в твоем коде есть константы, которые не меняются на протяжении выполнения всей программы, - не делай лишние присваивания. Например:

```
int x = 5, y = 7;
if (a < x && b < y)
  c = x;
```

лучше написать так:

```
if (a < 5 && b < 7)
  c = 5;
```

Таким образом, ты сократишь код, а также уменьшишь размер скомпилированной программы, сократишь время ее выполнения и освободишь память.

Совет #12

Избегай повторные вычисления одних и тех же выражений, достаточно сделать это один раз и в дальнейшем использовать полученное значение. Например:

```
if (a > x * 3)
  b = x*3 + (1 + x*3)/(100 + x*3);
for (int i = 1; i <= x*3; i++)
  c = i + b*x*3;
```

правильнее написать так:

```
y = x * 3;
if (a > y)
  b = y + (1 + y)/(100 + y);
for (int i = 1; i <= y; i++)
  c = i + b*y;
```

Это увеличивает скорость выполнения программы.

Совет #13

Внимательно следи за тем, чтобы в циклах не выполнялись операции, которые могут быть выполнены вне цикла. Например, в следующем примере:

```
For i = 1 to 1000
  x = x * 7
  y =y + i
Next i
```

операция x = x * 7 будет выполняться 1000 раз, хотя она свободно может быть выполнена всего один раз вне цикла, как показано в следующем листинге:

```
x = x * 7
For i = 1 to 1000
  y = y + i
Next i
```

Случаи, подобные первому примеру, сильно тормозят программу.

Совет #14

Чаще всего структуру выбора if лучше разделить на несколько блоков, например:

```
If x > 1 And y < 5 Then i = 0
```

можно разделить на два блока:

```
If x > 1 Then
  If y < 5 Then i = 0
End If
```

В последнем случае второй If не выполняется, если первый оказался ложным. Это способствует повышению скорости программы, т.к. исключаются лишние проверки. По тем же соображениям в структуре выбора if /else после оператора else всегда пиши то условие, которое менее вероятно может возникнуть в реальной ситуации.
В выражениях с операцией && (логическое И, в C/C++), если отдельные условия независимы, например:

```
if (x = = 0 && y > 1)
```

на первое место всегда записывай то условие, которое вероятнее всего окажется ложным, т.к. в этом случае анализ выражения будет сразу прекращен и передан следующей строке, что сокращает время выполнения программы. А в выражениях с операцией || (логическое ИЛИ), например:

```
if (x >= 1 || y >= 1)
```

на первое место пиши то условие, которое вероятнее всего окажется истинным.

Совет #15

Операции с элементами массива (индексными переменными) всегда выполняются медленнее, чем с обычными переменными. Поэтому операция a*b будет выполнена гораздо быстрее, чем a[i]*b[j], при одинаковых значениях. Следовательно, если необходимо использовать один и тот же элемент массива неоднократно, лучше присвоить его другой переменной и затем использовать ее. В циклах повышение производительности при этом может достигать 80 процентов.

Совет #16

Обращение к элементам одномерного массива всегда быстрее, чем к элементам многомерного массива. Поэтому всегда старайся использовать исключительно одномерные массивы, например, вместо матрицы 5 на 5 сделай одномерный массив на 25 элементов.

Совет #17

Не используй в своей программе рисунки в формате BMP. Надеюсь, тебе не стоит объяснять, что BMP требует много ресурсов и долго перерисовывается, лучше использовать такие форматы, как JPEG, PCX, WMF и др. Старайся также применять минимальное количество цветов, например, 16-цветный рисунок занимает половину требуемой памяти для 256-цветного рисунка, а монохромный - одну четверть памяти, требуемой для 16-цветного рисунка. Так, если у тебя рисунок содержит только белый и черный цвета, то правильным будет сохранить его как монохромный.

Совет #18

Если твоя прога долго грузится, используй заставку. Это, конечно, скорости программе не прибавит, но юзеру будет казаться, что она грузится быстрее. Только заставка должна быть простой, чтобы еще больше не тормозила загрузку. Пример простых заставок можно посмотреть в программах MS Office (как ни странно!).
С той же целью можно использовать и индикатор загрузки. Но если ты не можешь сделать так, чтобы он во всех случаях двигался равномерно, а не как часто бывает - рывками, лучше не делай, т.к. это создаст еще большее впечатление тормознутости программы.

Совет #19

Если ты не уверен в знании своего родного языка (а сейчас есть такая фича, что многие знают английский гораздо лучше, чем русский), то прогони свою программу в Word'е на проверку правописания. Это хотя бы минимально избавит ее от грамматических ошибок и "очепяток". Конечно, этот совет не относится к оптимизации, но грамотность в программах не менее важна, т.к. от тебя сразу все отвернуться, если увидят, например, вместо "Сохранить" - "Сохренеть" и т.п.

Это далеко не все советы, которые можно дать по оптимизации программ, а лишь их самая основная часть. Тем более по каждому отдельному языку программирования на эту тему можно говорить практически бесконечно. Поэтому я тебе дам последний - двадцатый - совет, чтобы ты действительно стал профессиональным кодером: прочитай хотя бы первый том (а всего их три) книги Дональда Кнута "Искусство программирования". Эта книга - настоящий мировой бестселлер, которую, считается, должен изучить всякий уважающий себя кодер. Кстати, сам Билли сказал, что кто прочитает все эти тома от корки до корки, может присылать ему свое резюме. Если ты умудришься таким способом попасть на службу к мелкомягким, то попытайся изменить Windows к лучшему :). Желаю удачи!

МУЗ ТВ

Вечерний звон

Наше

СИЕСТА...

Новости

shэйker

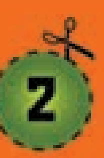
RUSSKIE

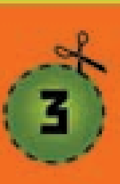
20

ВКЛЮЧИ МУЗ-ТВ – СМОТРИ МУЗЫКУ

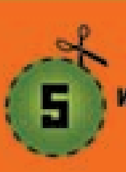














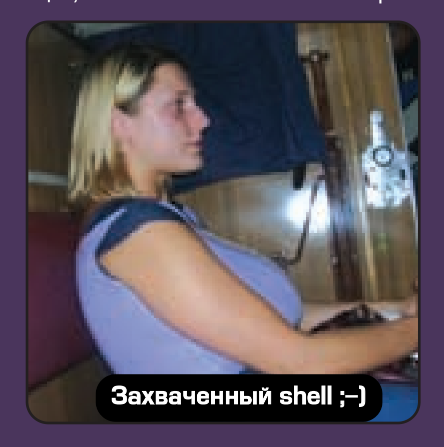
Конструктор Хаоса v 3.0

iCE DraGon // HellBender Group vs. SINtez & SideX // Gibbons Power Group :)

18-19 августа 2001 года в славном городе Санкт-Петербурге, в стенах кинотеатра "Восход" прошла одна из крупнейших в России деми-пати - Chaos Construction.

iCE DraGon
Наше путешествие на пати началось днем раньше, когда мы приехали на Ленинградский вокзал в Москве покупать билеты. Как выяснилось, билеты в кассах имелись в изобилии и по очень даже умеренным ценам. Билет в оба конца обошелся нам всего в 250 рублей (сидячие места в фирменном поезде), а проход на два дня пати стоил 100 рублей, то есть вся поездка могла обойтись москвичу всего в 600-700 рублей.

SINtez & SideX
Для нас пати началось еще в поезде :). Только мы успели погрузить свои тельца в вагон, к нам сразу же подошла миловидная девица с огромными г... глазами :). Таких больших глаз мы давно не видели. 6-й размер, точно! Слово за слово, и мы с подругой в вагоне-ресторане. Чай-кофе-потанцуем. В общем, часа в 3-4 ночи пьяный SideX перешел к

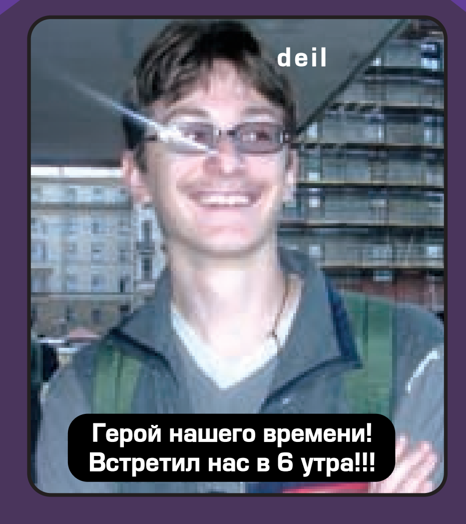

Захваченный shell ;-)

активному наступлению. В результате этой D.O.S. атаки Сайд открыл себе в Питере шелл, которым будет время от времени пользоваться :).

День первый

iCE DraGon
При входе мы встретили Ramzai и Amgorb из T-rex'а. Далее, пройдя вовнутрь, мы увидели сидящих на диванчиках оранжевых человечков. Это были Throb'ы и Night_//Neonray. Все в оранжевых комбинезонах, за которые их в дальнейшем все называли сотрудниками автомастерской.

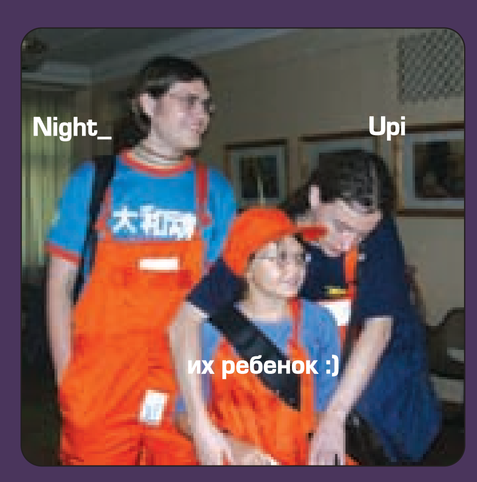
SINtez & SideX
Твою мать! Мазафакеры! Драные иносранцы! Все гостиницы забиты, бабки на вокзале предлагают какие-то хибары. Ладно, едем на пати с вещами. Полчаса в такси, и мы у кинотеатра. Народу-то! А вот и знакомые лица: T-Rex в основном составе (жаль, Танжа не было), мега-стильный Upi и Night_, Nap и другие личности. Заныкав коробку с призами и повесив наш баннер, мы с Сайдом уселись смотреть начало пати.



Герой нашего времени! Встретил нас в 6 утра!!!

iCE DraGon
Различные компо сменяли друг друга, народ тащился от комперов, которые выжимали из старенького Спеки все возможные ресурсы. Накладка произошла с ZX Spectrum 32kb Game. По техническим причинам часть игр не хотела корректно работать, и организаторы оперативно приняли решение проводить Amiga/PC Multichannel traditional and alternative music, дабы взять время на отладку.
В Amiga/PC Multichannel Traditional music явным лидером стал Serpent//HBG с композицией "Awakening!". "Stacy" от LAV//SandS ласкала ухо слушателя своей мелодичностью, но в ней было той экспрессии, которая была в "Awakening!". Сильно выделялась среди большинства работ "In Memory Of...", написанная maniak//TeC. Лично мне она понравилась наряду с композициями, занявшими первые места.
Среди композиций, представленных в Amiga/PC Multichannel Alternative music, выделялись работы: Amgorb//T-rex "TAHKu EDyT HA MAHEBPbI" и EA//Antares "Ruthless". Также неплохо звучали работы "Urban Pressure" от DeeGreez//TeC и "Just Happy Hardcore" от Buzzer. Но как бы там ни было, Amgorb//T-rex был лучшим в данной номинации, за что и получил первое место.
Далее началось долгожданное ZX Spectrum 32kb Game, которое все ждали с нетерпением. Было показано четыре работы, одна из которых - внеконкурсная. Первая игра была "Hunt on sparrows. Born to kill." от Green Bit Group, представлявшая собой пошаговый квест с видом от первого лица. Второй игрой была "Arcanoid" от Drv53b6//Phantom Family (название игры говорит само за себя). Третьей была показана "Farspace" от Mayhem. Ни в первой, ни в третьей игре никто ничего понять не смог. Самой интересной нам показалась внеконкурсная работа - ремейк игры Dizzy. Если бы работа участвовала в конкурсе, она бы обязательно заняла первое место.

SINtez & SideX
В 4 часа мы уехали с пати, нас ждали Даня Шеповалов, прогулки по Питеру и поиски жилья. К 8 вечера мы были такими уставшими, что SINtez



заснул прямо в машине. Нам все-таки удалось найти гостиницу, и через час мы стали "морячками" :). Потому что это была "гостиница моряков" в порту. WOW! Такого шлюшонистого места мы еще не видели. Проституция в этой гостинице абсолютно официальна. Впрочем, это правильно. Все-таки моряки, дальние плавания, сексуальный голод. Их можно понять. А заодно можно оправдать администрацию отеля, меняющую деньги проституткам после отработанного часа и продающую им же презервативы.


AMIGA CORE

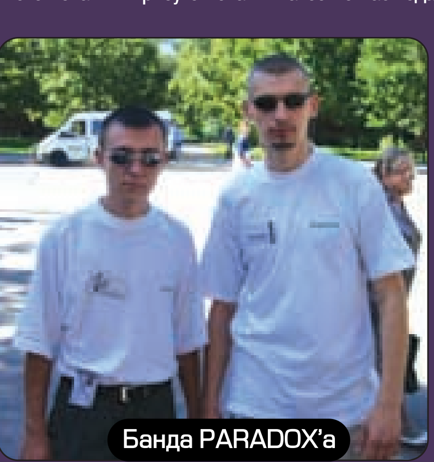


Наконец-то можно поспать! Как же, размечтались. Поспать нам удалось всего 2 часа, т.к. в полночь мы встречались с Даней для совместного похода в клуб "Метро". Там же, в клубе, мы встретили почти всю группу HBG, которая была такая же обколбашенная и сонная. Массовые возлияния алкоголя, и мы снова в седле.

День второй

iCE DraGon

На утро второго дня всех спящих в зале разбудили около половины восьмого, что вызвало немало недовольных выкриков со стороны внезапно разбуженных. Как выяснилось позже, зал надо было приводить в порядок для проведения религиозного обряда местной секты "Свет Миру", которая должна была начать акт просвещения в девять часов утра. В зале разрешили остаться нескольким людям, доделывающим свои работы, и организаторам пати. Программистам разрешили бить по кнопкам только во время песнопения и наложили строгое табу на программирование во время "внушения". После чего господа сектанты водрузили на сцену деревянный крест, и действо началось. В зале остался также Broken//HBG, который сильно хотел спать и присутствовал в качестве наблюдателя/потенциального члена секты. Позже он признался, что такой серьезной атаки на головной мозг он еще никогда не испытывал и в конце обряда был даже готов пожертвовать денег наряду с другими сектантами. Из зала периодически выбегали активисты секты, которые агитировали сценеров присоединиться к их рядам, на что сценеры предлагали сектантам влиться в ряды российской демосцены. В итоге стороны не пришли к согласию по данному вопросу, и где-то к половине двенадцатого, уже после истечения времени, отведенного сектантам, часть организаторов (Lav//Sands, Megus//BW и B-reeze//Fishbone) включили на полную громкость хардкор от Dioxide//HBG, после чего начали скакать по сцене, изгоняя таким образом злых духов, чем привели остатки сектантов в шок. Именно этим знаменательным событием было дано начало второму дню фестиваля, в течение которого были проведены оставшиеся Amiga/PC конкурсы. Но первым был проведен конкурс ZX Spectrum Demo, который все смотрели с большим удовольствием.


Банда PARADOX'а

SINtez & SideX

6 часов утра. Выходим из "Метро". В 6-30 плюхаемся на койки. Оба выставляем в мобайлах будильники на 10 утра, нужно прийти на начало второго дня, т.к. второй день посвящен Amiga/PC. Благополучно просыпаем все на свете и одновременно резко вскакиваем в полдвенадцатого. "Проспааааали!!!!" Сайд вальяжно бредет умываться. "Сайд! Хорош ползать! Давай в темпе вальса!" Через секунду SideX ускоряется до первой космической скорости, и все умывки/подмывки/сборы/завтрак укладываются в 10 минут. В полпервого мы на пати, абсолютно отмороженные, зевающие и вставляющие спички в глаза, встречаем полуживого iCE DraGon-а в таком же состоянии.


группа захвата KFC готовится к штурму

Долгожданные демки

iCE DraGon

В 64kb intro Amiga/PC была представлена всего одна работа "Robo" от иностранной группы RMM Design. Она была показана вне конкурса.

В номинации Amiga/PC 4kb intro было показано четыре работы, комментировать их не буду, лучше самим скачать и посмотреть.

В Amiga/PC Demo, несомненно, лидером стала работа от Critical Ma$$ "NucleaR ParadisE", сочетавшая в себе не только хорошо составленный сценарий, а также музыку, задававшую атмосферу всему творению, но очень красочные заставки между сценами, которым могли позавидовать графические конкурсы. "Demoscene - Dobro!" от Sigma Group представляла собой wildvideo с "демо-заставкой" в начале. Throb'ы представили промо-версию своей новой работы "Detroit PM 318", по которой можно судить, что готовится нечто грандиозное. Последним было показано творение от группы Fishbone "No fate", созданное с применением технологии флеш.

SINtez & SideX

Да... Это, конечно, не то, что мы ожидали. Реально крутых дем не было. А нам так хотелось подарить кому-нибудь наш главный приз - DVD-ROM. Очень понравилась работа от Throb, но это была не дема, а только реклама будущей демки. Поэтому, посовещавшись, мы решили "либо никому вообще, либо тем, кто сделал угарное видео". Так и получилось. Да, Sigma сделала не дему, это видео, что бы там в начале ни было. Но зато какой угар! Все, кто сидел в зале, выпадали в осадок от смеха. Нам это напомнило наш любительский видео-ролик, который ты мог видеть на CD к новогоднему Сервиспаку X. Еще мы протащились от mp3 композиции Мегуса, за что вручили ему второй приз - 3 CD с звуковыми сэмплами. Блин, ребята, эту композицию надо слышать! Такую песню можно прям хоть сегодня на радио выставлять, настолько профессионально сделано! Ну вот и все, призы раздали, пати закончилось, можно отдыхать. Поехали громить KFC (семнадцать голодных демщиков/тусовщиков в одном маленьком кафе - это рулез :).



съемка скрытой камерой: T–Rex продает пакет акций Zlobware

HACK-FAQ

Horrific (hack-faq@real.xakep.ru)



Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :)

Q: Установил на компьютер, который входит в одноранговую сеть из трех машин, систему Windows 2000. А проблема вот в чем: две другие машины не видят из сети мои диски (доступ я открыл полный и всем, система всех дисков FAT32), а при попытке обращения к ярлыку моего компьютера (из сети) появляется запрос на ввод пароля. При установке системы я вводил лишь пароль администратора (под ним и работаю), но при его вводе выдается сообщение об ошибке ввода пароля.

Там уже есть для тебя учетная запись "guest". Войди в ее свойства и убери флажок с "Отключить учетную запись". Потом задай пароль (щелкни правой кнопкой по учетной записи и выбери "Сменить пароль"). Теперь твои кореша смогут увидеть твои диски, если введут имя "guest" и пароль, который ты задашь.

Q: Действительно ли защита Windows 2000 надежнее и безопаснее NT?

Очень жаль тебя огорчать, но это так. Win2k действительно работает надежнее, и безопасность здесь уже на уровне. Только второе действительно в случае работы в нормальном режиме. Windows 2000 может работать в двух режимах: смешанный и "нормальный". При первом режиме используется старая и дырявая авторизация NT. В этом режиме ОСь работает по умолчанию, чтобы сохранить совместимость со старыми ОСями. Во втором режиме используется уже проверенная в *nix авторизация по kerberos. Поэтому, если MS не внесла здесь своих изменений, то Win 2000 может получить крутость nix-ов.

Q: Я немного запутался. Некоторые ругают MS SQL Server за плохую защиту, а некоторые наоборот хвалят. Кому верить?

Сам по себе SQL сервер великолепный, и я им активно пользуюсь. Но у него действительно есть два недостатка. Во-первых - это учетная запись администратора. По умолчанию имя пользователя это "sa", а пароль пустой. Некоторые программеры и администраторы по вине своей лени оставляют эту запись без изменений. Поэтому нет никаких проблем получить полный доступ. Лично я не считаю эту дыру виной MS, потому что это вина админов. В Sybase дыра еще больше, там пароль хранится в открытом виде в реестре. В SQL Server 2000 заложена атомная бомба. Для получения доступа можно использовать авторизацию самой Windows 2000 и авторизацию SQL сервера. Вот это мне кажется дырой побольше. Во-первых, это значит, что для входа в базу есть две двери. А найти ключик к одной из двух легче, чем к одной. Во-вторых, SQL сервер будет подвержен не только своим дырам, но и дырам в авторизации Windows 2000.

Q: Что такое сети/подсети классов C и B? И чем отличаются?

Адреса сети класса B начинаются с "10", а адреса сети C начинаются с "110". IP адрес делится на две части: адрес сети и адрес узла в сети. Класс IP адреса говорит о том, сколько байт относится к адресу сети, а сколько к адресу узла. В адресах класса B адрес сети занимает 2 байта и адрес узла тоже 2 байта. В адресах класса C адрес сети занимает три байта, а адрес узла 1 байт. Если ты силен в математике, то тебе этой инфы должно быть достаточно, чтобы понять суть. А именно: в сетях класса B может быть 65 тыс. уникальных сетей и столько же узлов. В классе C узлов может быть только 255, зато таких сетей можно нагородить ...

Q: Может я задам ламерский вопрос, но как узнать свой IP, HOST и порт?

Про то, как узнать свой IP, мы уже писали много раз. Так что вынь из ушей бананы или что там у тебя. Для этого есть утила Winipcfg.exe. Находится она в дире, где у тебя расположен Windows. Только вот я не могу понять, что означает "как узнать свой HOST". Хост - это в принципе компьютер, к которому ты подключаешься. Так что он не может быть твоим. Как узнать свой порт? Так у тебя их просто громадное количество. Например 1, 2, 3... 3000, 3001... Это все твои порты. Столько, сколько волос на голове. Так что узнать их невозможно. А насчет ламерского вопроса дам тебе совет. Если не хочешь выглядеть ламом, то заглядывай сначала в словарь (например, Lingvo). Запускай там поиск по слову Host, и ты уже не будешь выглядеть ушастым ламом :).

Q: Если я на ftp сделаю файлу chmod execute - что это значит? Запускать файл на сервере или что? HELP PLZZ

Ну, конечно же, ты меняешь атрибут файла и даешь право на его исполнение. После такой операции файл можно запускать. Только не каждый сервер позволит тебе делать такие манипуляции.

Q: Yo Horrific (ну или кто там у вас на вопросы отвечает?) Мой вопрос: как узнать диапазон IP-шников моего прова?

Yo. Да ты проснулся. Народ уже давно научился пользоваться сервисом WHOIS. А ты где был? Пиво пил? Смотри, в компании с толстяком всю жизнь пропьешь. Самый простой и в то же время очень точный способ. Заходишь в iNet и запускаешь winipcfg.exe. Запомни свой IP. Потом идешь на www.ripn.net. Там есть сервис WHOIS. Щелкаешь. Запускаешь поиск по своему IP, и сервер тебе показывает, кому он принадлежит, какой диапазон зарегистрирован и все такое. Так что хватит пить пиво, пора есть мясо.

Q: По какому принципу работают порт сканеры?

Простой коннект на порт. Если коннект удачен, то порт открыт. Если никаких ответов на коннект нет, то порт закупорен. Все гениальное просто.

Q: Снова вопрос про порт сканеры. А как проверить открытый telnet порт? Ведь без пароля к нему нельзя приконнектиться.

Ты подумал, что ты сказал? Как я вижу, нет. Как у тебя могут запросить пароль без предварительного коннекта. Протокол соедине-

ния действует так.
1. Сначала происходит попытка соединения.
2. Ответ на попытку.
3. Обмен служебной инфой.
4. Запросы паролей или другой дребедени.
Без коннекта невозможен запрос пароля. Так что любой, даже защищенный порт откликнется, только если на нем не стоит Firewall.

Q: У меня на винте была компрометирующая меня инфа (я с голыми девками :)). Я ее потер, но существуют проги, которые ее восстановят из вусмерть заформатенного винта. Дай совет, как ее потереть по-настоящему (только не уничтожая другую)? Пиво послать не могу, пока дойдет - несвежим будет.

Сделай дефрагментацию, во время нее большинство секторов перемещаются, и твои стертые данные затрутся с вероятностью 70% (зависит от заполненности твоего винта). Можешь еще скопировать несколько раз куда-нибудь большие файлы, а лучше забей весь винт инфой и несколько раз перегрузись, тогда очистятся не только кластеры, но и файл подкачки. Конечно же, есть проги, окончательно уничтожающие файлы (читай про них в этом же номере), но ручное затирание эффективнее :). А насчет пива не волнуйся. Высылай в холодильнике :). Мы с удовольствием собираем любые охлаждающие агрегаты, чтобы потом продавать их под своей маркой. Так что ожидайте скорого выхода на прилавки города холодильного агрегата для пива под маркой][. Надо же куда-то сплавлять заработанные холодильники.

Q: Как полазить в компьютере друга, чтобы в логах ничего не осталось? На компьютере друга установлена Win 98, Internet Explorer 5, Office 2000, остальное игры.

Все... С сегодняшнего для ухожу на покой. Я все понимаю, но с каких это пор в Windows 98 есть логи? Наверно я отстал от жизни и за три года юзанья Win98 не разу не заметил логов. А может быть мои глаза до такой степени налились пивом, что я не соображаю уже? И вообще, главред обязан бесплатно отправить меня лечиться в лучшую психиатрическую лечебницу. Можно даже пожизненно, потому что у меня от возмущения пена изо рта пошла. А это уже первый признак сумасшествия.

Q: Проблема такая - 98 не определил мой ATX! Не знаю, что делать. Я переустановил Win еще разок, но никаких изменений не произошло. Да еще вдобавок 98 и сидюк не определил. Так что ни CD, ни ATX. Стоит заметить, что перед этим я ставил сначала W2K, а потом Me. И после этого все полетело. И лампочка, которая показывает обращение к винту, постоянно горит, даже если я ничего не запустил, и вообще ни хрена не делаю. В общем, полный капут.

А у меня Win 98 не определил коврик для мыши и постель для монитора. Так что теперь у меня коврик лежит без движений и лампочки больше не горят. ATX это, грубо говоря, формат или размер матери и, соответственно, тип корпуса. У тебя что, Win98 не определил размеры корпуса? Наверно ты неправильно что-то замерил линейкой или не то указал в настройках. Попробуй изменить параметры ATX на AT, может поможет :). Судя по всему, если не определен сидюк, у тебя проблемы с матерью. ATX тут не причем и ME и W2K тут не причем. Просто ты, наверно, забыл установить какие-то дрова под мать. Скажи, какая мать, и, возможно, я помогу тебе. В любом случае CD-ROM можно подтянуть вручную, добавив его в autoexec.bat и config.sys. В общем, пиши, объясню.

Q: Прочитал статью про взлом CGI, а в .php и .asp такие же дырки или нет?

Абсолютно такие же. Главная проблема программеров сайтов - неумение проверять входную инфу. Большинство использует переданные формой данные без проверки. А если это так, то ты можешь переслать что угодно. Иногда таким образом можно добиться многого.

КИБЕРСПОРТ

Компьютерные игры признаны официальным видом спорта

Александр '2poisonS' Сидоровский (2poisonS@real.xakep.ru)

В нашем календаре много праздников – понятных и непонятных, нужных и ненужных, отмечаемых и не очень. Если тебе все эти дни конституции-независимости-шахтера-вахтера глубоко параллельны и из всех "красных дней календаря" ты вынес только две традиции: напиться на Новый год и помыть посуду на 8 марта – приготовься включить в список праздников еще одну знаменательную дату: 25 июля.

Именно в этот день в 2001 году Россия стала первой в мире страной, где компьютерные игры официально признаны видом спорта, наряду с футболом, шахматами или, скажем, теннисом. Об этом говорится в приказе №449 Государственной Российской Федерации по физкультуре, спорту и туризму. То есть, как видишь, официальней уже некуда.

Можешь себе представить, как это событие отразилось на игровой общественности. Прикинь, сколько нужно всего сделать, чтобы компьютерные игры получили такое же распространение, как, скажем, футбол. Нужно организовывать секции, писать целые тома всяких правил, нормативов и прочей сугубо бюрократической ерунды, чтобы "отцы", "папы" и "гуру" превратились в кандидатов и мастеров спорта. Вся эта титаническая работа легла на плечи Федерации Компьютерного Спорта (ФКС) России - можешь себе представить, какая у них сейчас там запарка. Однако народ должен знать своих героев, и поэтому нам удалось вытащить на интервью (несмотря на всю его занятость) ни много ни мало генерального секретаря ФКС России Константина Сурконта. Он-то и прояснил всю эту ситуацию с официальным признанием, которая поначалу казалась нам слишком неправдоподобной и подозрительной (SINtez так вообще решил, что это утка).

X: Для начала определимся, что же все-таки произошло. Расскажите об этом таинственном "приказе №449". Кто, кому и что приказал? В чем суть случившегося?

Благодаря приказу N449 от 25 июля 2001 года компьютерные игры включаются в перечень видов спорта, рекомендованных для введения в государственные программы физического воспитания населения России.
Таким образом, Россия становится первой в мире страной, признавшей компьютерные игры официальным видом спорта.

Lenta.ru 27.07.2001

КС: Официальный текст приказа, вернее выдержка из него, звучит так: Включить в перечень видов спорта для введения в государственные программы физического воспитания населения и рекомендуемый для развития в Российской Федерации компьютерный спорт как (дисциплину) вид спорта. Подписал приказ П.А. Рожков - Председатель Государственного Комитета Российской Федерации по физкультуре, спорту и туризму. Приказ датирован 25 июля 2001 года.

На некоторых сайтах была ошибка. Вместо июля писали июня. Это лично моя вина, которую я по возможности попытался исправить. Все дело в том, что я решил запостить такой ньюз сам и от радости не проверил тщательно. Ошибся, а потом разослал URL по всем, кто есть в моем ICQ. И только к вечеру заметили ошибку. Потом часа три ушло на то, чтобы отыскать все сайты, где инфа уже пошла, и извиниться перед всеми авторами статей.

Так что 25 июЛя можно с уверенностью считать днем рождения компьютерного спорта! :)) Или, если угодно, киберспорта. В следующем году мы к этой дате приурочим
какой-нибудь крупный турнир. Скорее всего, это будет Кубок России.

Если коротко, то с этого дня компьютерный спорт является официальным видом спорта в России. Таким же, как все виды спорта, существующие на сегодняшний день. Он чем-то
напоминает шахматы и шашки, но в то же время похож на технические виды, такие как автомобильный спорт, где человек управляет механизмом. Ну а если судить по массовости, то тут он может сравниться с футболом и хоккеем.

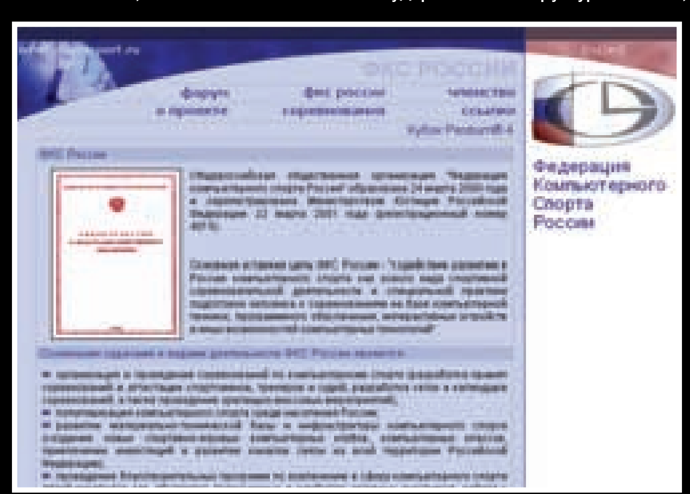
Он рекомендован для развития в Российской Федерации, по нему присваиваются разряды и сдаются нормативы. Открываются секции компьютерного спорта, где юные
киберспортсмены тренируются делать рокет-



джамп и защищаться тоссами от зергов:)), а также постигают разницу движков ку3 и анрила и их взаимодействие с третьим гефорсом.
Преподается история компьютерного спорта, начиная с Дума и Варкрафта, подробно изучается тактика командной игры на примере экшенквейка, каунтера и фифа2000. Мамы и папы приводят своих чад к платным индивидуальным преподавателям, а те впаривают (то есть рекомендуют) им мышки и клавиатуры, лучшие для такого размера руки. И ни в коем случае нельзя брать мышку на вырост :)).

Но если серьезно, то ничего смешного нет. Это несколько необычно, но, если вдуматься, то закономерно. Чтобы стать настоящим спортсменом в этом виде, надо много иметь от
рождения и очень многому научиться. Профессиональный спорт здесь, как и везде, тяжкий труд, а любительский служит гармоничному развитию личности. Тренировка
концентрации, умение предугадать поведение противника, сыгранность команды и дух соревнований - атрибуты спорта, и с этим сложно спорить.

Х: Какое отношение ко всему этому имеет ФКС? Каковы будут ваши функции? Почему именно вы?
КС: ФКС России - Общероссийская общественная организация, созданная в соответствии с Федеральным Законом о спорте при поддержке Госкомспорта России и зарегистрированная Министерством Юстиции РФ. Как и в любом другом виде спорта, в компьютерном спорте существует единственная общественная спортивная организация, аккредитованная при спортивном комитете, разрабатывающая нормы и правила проведения соревнований, присвоения разрядов, аттестации судей и тренеров.
Я встречал на многих веб-сайтах такую фразу: "На роль главной управляющей общественной структуры новой спортивной дисциплины претендует Федерация компьютерного спорта России". Это не совсем так. Любой вид спорта, а особенно компьютерный спорт, настолько широк, что мы просто не в силах взять под контроль все, что будет в нем происходить. Но по мере возможности ФКС России готова оказать поддержку любому проекту, любому начинанию, развивающему и пропагандирующему компьютерный спорт в России и в мире, причем поддержку на самом высоком уровне. При условии, конечно, что этот проект не принесет никому вреда. Спорт, в первую очередь, призван воспитывать лучшие качества в человеке и объединять общество. Компьютерный спорт не исключение.
Небольшая ремарка к слову "претендует". Не могу это пропустить. В какой-то мере этим словом нарушается логика причинно-следственной связи. Конечно, компьютерный спорт
существовал до его официального признания. Но вы только попробуйте представить, какие нужно было составить документы, как тщательно прописать правила присвоения
разрядов в компьютерном спорте, положение о соревнованиях и программу обучения компьютерному спорту, чтобы Государство признало его спортивной Дисциплиной. Такая
работа была выполнена нашими специалистами впервые в Мире. За это им всем респект, как говорится. Никто ни на что не претендует. Мы просто это сделали! И огромное
спасибо всем, кто нам в этом помог! И государственным структурам - за то,





что осознали необходимость такого признания, и самим спортсменам - за то, что играли и развивали само движение. А еще попробуйте представить, какая образовалась коммерческая ниша в этой области и как активно она сейчас начнет разрабатываться.

Х: А что вообще такое ФКС? Расскажите о себе. Когда возникла Федерация, чем вы занимаетесь в настоящее время, есть ли аналогичные организации в России? Если вам действительно выпадет ведущая роль в развитии официального киберспорта, во что трансформируется ФКС?

КС: Общероссийская общественная организация "Федерация компьютерного спорта России" была образована на учредительном съезде 24 марта 2000 года и зарегистрирована 22 марта 2001 года (рег. номер 4015). Для регистрации нам понадобился целый год! Зарегистрировать спортивную федерацию по виду спорта, которого де юре не существует, знаете ли, сложно :)). Сегодня в составе ФКС России 56 региональных отделений.

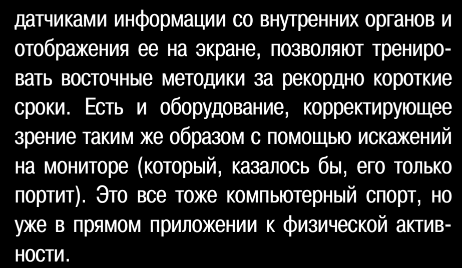
Но, судя по тому, как активно откликаются регионы на идеи развития компьютерного спорта в России, скоро мы заполним все 89. Аналогичных организаций нет не то что в России, нет в мире! Отвечу и на вторую часть вопроса. Вполне возможно, что, когда говорится о ведущей роли в развитии официального киберспорта, имеется в виду не развитие в России, а развитие в мире. Сегодня мы инициируем создание подобных организаций в других странах. ФКС России не будет никуда трансформироваться. Но, я искренне надеюсь, что при нашем непосредственном участии и с нашей подачи будет образована Международная спортивная федерация. Будет ли включен компьютерный спорт в Олимпийские виды? Да. Слишком много людей им занимается. Но это уже другая история, которая займет не год и не два.

Х: Первое, что приходит в голову, когда читаешь текст приказа 449, - "неужели теперь компьютерные игры будут преподавать в школе?" Наверное, до этого еще далеко, а вот что насчет специализированного спортивного обучения? Ведь теперь это должны быть не просто игровые клубы, а настоящие спортивные секции, с тренерами, расписаниями занятий и т.д. Будет ли это?

КС: Да. В общеобразовательных школах - не знаю. Есть инициативные преподы, которых киндеры любят и уважают, но есть и злые завучи, которые все новое воспринимают в штыки. А вот специализированное образование будет. Российские киберспортсмены на сегодняшний день, попросту говоря, рулят. Кто в мире может сравниться с Полосом, Повером, Асмой или Гостом? Единицы. Но чтобы продолжать традиции, надо тренироваться и тренировать других. Школы киберспортивного мастерства и секции компьютерного спорта нужны, если мы не хотим потерять тот престиж, которого достигли на энтузиазме.

Х: Какие еще мероприятия предусматривает "государственная программа физического воспитания населения"? Расшифруйте эту фразу.

КС: Программа физического воспитания населения подразумевает выделение государственного финансирования на физическое воспитание граждан России и определенные льготы предпринимателям в этой области. Как связан компьютерный спорт с физическим воспитанием? Именно вашему журналу, как наиболее технологичному и прогрессивно-андеграундному :)), открою маленькую тайну. Компьютерный спорт - не только мышь, клавиатура и монитор. Есть и другие, буквально завораживающие перспективы. Интерактивные тренажеры, например. Сегодня есть такие. Гольф с реальной клюшкой, в котором компьютер рисует полет мяча на огромном экране (разумеется, на фоне ландшафта). Или комнаты, в которых стены, пол и потолок - мониторы, а человек внутри в шлеме и с навороченным девайсом в руке уворачивается от виртуальных монстров. Есть просто тренажеры, которые, за счет считывания



датчиками информации со внутренних органов и отображения ее на экране, позволяют тренировать восточные методики за рекордно короткие сроки. Есть и оборудование, корректирующее зрение таким же образом с помощью искажений на мониторе (который, казалось бы, его только портит). Это все тоже компьютерный спорт, но уже в прямом приложении к физической активности.

Я уж не говорю о том, что в программу физического воспитания населения входят военно-патриотические спортивные игры и тренировка поведения в экстремальных условиях. А каких классных специалистов можно сделать из команды игроков, которые сыгрались по Инету, не видя друг друга в лицо и даже не слышав ни слова друг от друга.

Х: Любой спорт имеет систему разрядов. Если к чемпионатам по компьютерным играм мы все привыкли, то словосочетание "мастер спорта по Квейку" звучит, по крайней мере, необычно. Определены ли спортивные разряды для компьютерных игр? Если да, то какие и как их получить?

КС: Вся информация об этом находится у нас на сайте www.cybersport.ru в разделе "Соревнования". Там действительно есть разряды вплоть до мастера спорта международного класса. Ну, конечно, не по квейку :)). А то бы ID-шники нам бы денег должны были немало :)). Нет, там все очень разумно. Игры разделены на классы, в которых начисляются баллы, и, соответственно, присваиваются разряды.

Х: Какие чемпионаты, турниры, соревнования будут проводиться на официальном уровне? Как попасть на них в качестве участника?

КС: Это все там же. Чемпионаты федеральных округов (для тех кто не знает, в России их семь, и каждый по площади больше Европы :)), Кубок России, Открытый Чемпионат России и Суперкубок. Но и все, кто хочет, могут проводить соревнования сами при нашей поддержке. Для придания таким соревнованиям статуса спортивных достаточно выполнить ряд общих требований.

Х: Допустим, я новичок в компьютерных играх, но очень хочу овладеть искусством мышки и джойстика. Куда мне пойти, к кому обратиться, по какому телефону позвонить, чтобы меня приняли "на обучение"? Сколько это будет стоить?

КС: :)) С этим пока сложно. Ведь только-только все началось. Но посмотрим, что будет через месяц. Уж желающих обучать за деньги найдется немало :)).

Х: Теперь предположим, что я - опытный игрок в Каунтер-Страйк. За плечами множество побед, и все друзья смотрят на меня с завистью. Хочу в большой спорт. Вопрос тот же - куда идти, где расписаться? :)

КС: Участвовать в рейтинговых (спортивных) соревнованиях. Часть прошедших мы

Мастер спорта международного класса

А. Присуждается спортсмену, занявшему 1-2 место на Открытом Суперкубке России, при условии участия в соревнованиях по данному классу игр спортсменов не менее чем из 8 зарубежных стран (в том числе не меньше чем из двух ведущих в области компьютерного спорта стран: США, Германия, Швеция, Великобритания), и имеющему разряд не ниже Кандидата в мастера спорта.

Б. Присуждается, в случае создания признанной спортсменами ведущих стран международной организации по компьютерному спорту, спортсмену, занявшему 1-2 место на официальных чемпионатах континентов или занявшему 1-3 место на официальном чемпионате мира или Олимпийских играх по видам компьютерного спорта.

Мастер спорта

Для мужчин:

Присуждается спортсмену, занявшему 1-3 место на чемпионате России в дуэльных соревнованиях или в составе команды в командных соревнованиях, при условии наличия не ниже первого разряда.

Для женщин:

Присуждается спортсменке, занявшей не ниже 7 места на чемпионате России в дуэльных соревнованиях или в составе команды в командных соревнованиях, при условии наличия не ниже первого разряда.

Кандидат в мастера спорта

Для мужчин:

Присуждается спортсмену, занявшему не ниже 6 места на чемпионате России в дуэльных соревнованиях или в составе команды в командных соревнованиях, при условии наличия не ниже третьего разряда.

Для женщин:

Присуждается спортсменке, занявшей не ниже 10 места на чемпионате России в дуэльных соревнованиях или в составе команды в командных соревнованиях, при условии наличия не ниже третьего разряда.

Из "Перечня разрядов по компьютерному спорту" www.cybersport.ru





можем также признать рейтинговыми все с теми же условиями, определенными Положением о соревнованиях. Да, возможно в этом году кто-нибудь получит и Мастера спорта. Увидим в декабре.

X: Выходит, Россия хотя бы в чем-то первая! И не в чем попало, а в такой хай-тековской области, как киберспорт. Вам уже известна реакция западных игровых организаций и вообще - "широкой общественности"? :) Что думают - считают нас сумасшедшими или завидуют? А может, теперь стоит ожидать волну официальных признаний компьютерного спорта по всему миру? И если так, может ли Россия как пионер кибердвижения рассчитывать на роль мирового центра спортивных компьютерных игр?

КС: Буржуи пока не просекли. На Украине, в Белоруссии, Молдавии и Казахстане народ потихоньку просыпается. В Китае - завидуют. У них с этим сложнее. Все только по решению Партии :)). Вот и до Прибалтики волна дошла. Ждем.

А вот роль центра - это должно стать нашей целью. Когда мы создадим международную киберспортивную федерацию (с названием я пока не буду торопиться), нужно будет приложить все усилия к тому, чтобы ее штаб-квартира оказалась в Москве. Только тогда мы сможем остаться центром киберспорта.

X: Наверняка мы не задали вам хотя бы один вопрос, на который вы хотели бы ответить. Возможно, у вас есть какая-то дополнительная информация, или вы просто хотите сказать что-то читателям Хакера.

КС: Наверняка :)). Но уже семь утра, и пора спать. Я думаю, что это не последнее интервью. Спасибо вам за подборку хороших вопросов. Это огромная помощь для меня. А то многие просят мало того что дать интервью, так еще и вопросы самому написать. А нам сейчас, конечно, надо как можно больше придать огласке факт признания компьютерного спорта. А то получится как с Гагариным. Сейчас-то вроде и неясно, кто первый летал. Мы-то с вами знаем, а вот дети... В общем, спасибо.

А читателям Хакера хочу сказать очень много. Особенно после того, как мне какой-то умник линию запараллелил телефонную.
На самом деле, никогда не бойтесь непреодолимых препятствий, их нет. И ничего не считайте данностью. Реальность можно изменить, сделав, казалось бы, невозможное. Надо только постараться.





В декабре этого года в Сеуле состоится игровой чемпионат под названием The 1st World Cyber Games с призовым фондом в $300,000. В этом событии примут участие более 350 игроков из 25 стран мира. В данный момент национальные отборочные туры проводятся в игровых клубах 18 российских городов: Краснодаре, Самаре, Нижнем Новгороде, Екатеринбурге, Новосибирске, Иркутске, Владивостоке, Волгограде, Ростове на Дону, Тюмени, Томске, Челябинске, Воронеже, Красноярске, Ижевске, Калининграде, Санкт-Петербурге и Москве. Российский финал пройдет 8-14 октября в Москве. Примечательно то, что российский этап чемпионата организует компания Samsung, являющаяся мировым партнером World Cyber Games. Представители компании подчеркивают, что компьютерные игры на данный момент - не просто мимолетное увлечение, а «динамично развивающаяся часть мировой культуры», что кибер-спорт становится все больше похож на спорт традиционный и компания стремится привнести в чемпионат благородный спортивный дух.
Из шести официальных игр World Cyber Games 2001 года в российском отборочном туре участвуют три: Q3 Duel, Q3 Teamplay и Counter-Strike. Между победителями в этих номинациях распределяется призовой фонд в $50,000, в то время как на сеульский финал полетят только одержавшие верх в Q3 Duel и Counter-Strike. Ознакомиться с правилами и регламентами, а также зарегистрироваться для участия в чемпионате, вы можете на официальном сайте World Cyber Games: http://www.worldcybergames.ru.

С шотганом под юбкой
Размышления девчонки, которая стала геймершей-по-жизни

Лиса (vixen@xakep.ru)

Я девушка. Возможно, по твоему мнению этого достаточно, чтобы исключить меня из круга людей, с которыми ты стал бы обсуждать компьютерные игры. А зря. Думаешь, мы умеем только Cosmopolitan читать, сериалы смотреть и сплетничать? Тогда ты отстал от жизни, причем сильно.

Да, возможно, мы и не способны оценить весь кайф бессонной ночи, проведенной в лабиринтах с ракетницей наперевес или убитой на планирование и осуществление крупномасштабного наступления по всей линии какого-нибудь виртуального фронта. Есть, конечно, геймерши, способные с пеной у рта доказывать тебе, что шотган во второй Кваке на средних дистанциях очень даже ничего, но сейчас речь не о них. Речь пойдет о таких несовместимых на первых взгляд вещах, как твои любимые компьютерные игры и обычные, совершенно некомпьютерные девушки. Ты никогда не задумывался, что на самом деле твоя подружка совсем не такая уж ламер-girl, как кажется на первый взгляд? Нет? Значит либо она слишком хитрая, либо ты слишком наивный (или невнимательный?). Потому что мы (внимание, сейчас раскрою страшную женскую тайну! :)) очень часто играем с вами в разные игры, используя по сути те же самые тактики и приемы, которые ты юзаешь в своих контр-страйко-крафто-анрыловских упражнениях. Я могу честно рассказать тебе о некоторых из этих приемов (описать все просто невозможно), так как лично у меня время, когда я их активно (и небезрезультатно!) применяла, уже в прошлом. Мой бой-френд давно просек фишку, и мои маленькие хитрости потеряли всякий смысл.

Осторожно, засада!

 всех фанатов шутеров свой собственный стиль игры. Есть, например, кемперы, предпочитающие не носиться по уровням как Том и Джерри, а спокойно заныкаться где-нибудь в укромном уголке, методично отстреливая попадающих в поле зрения противников. Мы нередко применяем ту же тактику в своих отношениях с противоположным полом. Действительно, зачем тратить силы на активные поиски подходящей компании на вечер? Не говоря уже о том, что девушка, нарезающая круги по оживленной площади и пристально разглядывающая всех встречных парней, будет выглядеть по меньшей мере... своеобразно. Нам оно надо? Куда проще занять где-нибудь выжидательную позицию (ну, скажем, за столиком в каком-нибудь баре) и спокойно оценивать окружающих особей мужского пола на предмет... да чего угодно - начиная от невинного флирта там же за столиком и заканчивая безумным сексом на крыше соседнего небоскреба. Так что, зайдя в бар выпить пивка и увидев такую скучающую барышню, заранее продумай пути отступления (на случай, если она окажется не в твоем вкусе).

Так что если я безропотно соглашаюсь посмотреть с моим парнем новый супер-боевик, затем в течение двух часов наблюдаю, как он гамится в контр-страйк, периодически поднося ему ледяного пива, а потом еще сама развожу его на секс, он начинает готовиться к осаде - все это верные признаки того, что мне от него что-то нужно, и быстро.

Все для фронта, все для победы!

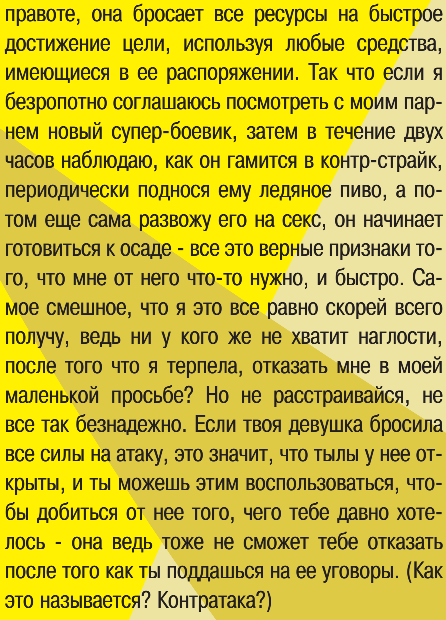
Если ты любишь стратегии, ты, конечно, знаком с тактикой rush'а. Только имей в виду, что твоя подружка тоже с ней хорошо знакома и, более того, наверняка успешно ее применяет. Как? Да очень просто. Я в свое время часто к ней прибегала и практически всегда с нужным результатом. Эффективна эта тактика, когда твоей красавице от тебя очень нужно что-нибудь такое, на что ты, скорее всего, не согласишься (например, пойти на день рождения к ее двоюродной тетушке. В костюме-тройке). Что делает твоя любимая? Понимая, что долгая дискуссия в такой ситуации лишь еще сильнее убедит тебя в твоей











правоте, она бросает все ресурсы на быстрое достижение цели, используя любые средства, имеющиеся в ее распоряжении. Так что если я безропотно соглашаюсь посмотреть с моим парнем новый супер-боевик, затем в течение двух часов наблюдаю, как он гамится в контр-страйк, периодически поднося ему ледяное пиво, а потом еще сама развожу его на секс, он начинает готовиться к осаде - все это верные признаки того, что мне от него что-то нужно, и быстро. Самое смешное, что я это все равно скорей всего получу, ведь ни у кого же не хватит наглости, после того что я терпела, отказать мне в моей маленькой просьбе? Но не расстраивайся, не все так безнадежно. Если твоя девушка бросила все силы на атаку, это значит, что тылы у нее открыты, и ты можешь этим воспользоваться, чтобы добиться от нее того, чего тебе давно хотелось - она ведь тоже не сможет тебе отказать после того как ты поддашься на ее уговоры. (Как это называется? Контратака?)

Палка, палка, огуречик – вот и вышел человечек!

РПГшники тоже могут увидеть немало знакомого в поведении своих подружек. Занимаясь генерацией персонажа, ты выбираешь те статсы и потом в процессе игры прокачиваешь те скиллы, которые наиболее важны с твоей точки зрения. Так же поступаем и мы. С той разницей, что раскачиваем мы не виртуального чара, а очень даже реального - тебя :) (Помнишь песенку - "Я его слепила из того, что было..."? Вот-вот, как раз в тему). Ты же, наверняка, не раз слышал от своей подружки ненавязчивые комментарии по поводу своих привычек ("Дорогой, ты выглядишь намного лучше, когда не ковыряешься в носу"), занятий ("Любимый, сидеть целыми днями за компьютером вредно для твоего здоровья"), внешнего вида ("Милый, ты уверен, что эта стрижка тебе действительно идет?"), друзей ("Что у тебя может быть общего с этими?.."). Все это выглядит на первый взгляд как забота о тебе, но на самом деле девушка занимается тем же увлекательным делом, что и ты, играя в РПГ - генерит персонажа. Тут для тебя самое главное - не позволить барышне посягать на святое. В конце концов, может, с другой стрижкой ты и правда выглядел бы не хуже (все-таки согласись, что в этом мы разбираемся лучше, чем в компьютерных играх), но вот растерять всех своих друзей, потому что твоей мадам не нравится музыка, которую они слушают... В общем, сам решай, что тебе дороже.

Мы (внимание, сейчас раскрою страшную женскую тайну! :)) очень часто играем с вами в разные игры, используя по сути те же самые тактики и приемы, которые ты юзаешь в своих контр-страйко-крафто-анрыловских упражнениях.



Sim–Sim, отдайся!

Еще один жанр, о котором нельзя здесь не вспомнить, - это всевозможные симуляторы. Само слово "симулятор" вызывает смутные ассоциации с прекрасной половиной человечества. Причем, так же, как в компьютерном жанре, в жизни симулировать можно все что угодно, и надо признать, мы частенько пользуемся этим в общении с вами для достижения своих целей. Примеров здесь уйма. Можно, скажем, симулировать болезнь, кстати, используем мы это в разных ситуациях. Если мне кажется, что мой парень как-то меньше внимания стал уделять мне и больше - компьютеру и друзьям, я могу, конечно, обидеться и вообще свести наше общение к периодическим случайным встречам в аське. Но могу пойти другим путем и изобразить легкий грипп (в особо запущенных случаях девушке придется симулировать полный паралич всех конечностей), и забота и внимание моего друга мне обеспечены (по крайней мере, на ближай-

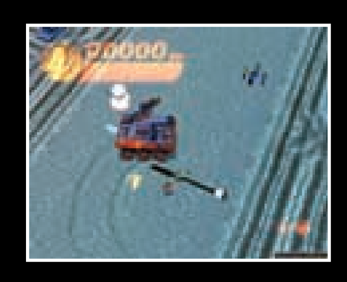


шую неделю). Твоя подружка может еще играть в симулятор болезни в случае, если ей не хочется посещать какое-нибудь мероприятие (например, футбольный матч или сборище всех твоих друзей-оболтусов). Есть еще менее очевидные для тебя случаи использования этого приема - предположим, твоя новая подружка решила сделать ваши отношения более близкими, а ты не проявляешь необходимой инициативы. Тогда постельный режим - это прекрасный предлог, чтобы продемонстрировать тебе новое сексуальное белье (а если ты достаточно догадливый, то и то, что под ним). Помимо болезни девушка может симулировать множество разных вещей. Вот пример из другой области. Когда ты на романтическом свидании взахлеб пересказываешь своей барышне содержание последней серии “Звездных войн” или рассуждаешь о том, какую материнку и сколько памяти тебе купить при предстоящем апгрейде, ты же всерьез не думаешь, что ее в этот момент действительно волнуют эти увлекательнейшие для тебя темы? Тем не менее, она слушает тебя, открыв рот. Как ты догадался, это - очередной сим. Дама симулирует интерес, чтобы показать тебе, что ты для нее - самый-самый, и ее безумно интересует все с тобой связанное. Мы очень часто используем эту тактику в начале отношений, пока бой-френд еще не в курсе наших реальных интересов. Кстати, на этом этапе у тебя есть неплохой шанс действительно подсадить подругу на свои увлечения проверено.



Вот, вкратце, те маленькие хитрости и уловки, которыми мы пользуемся, чтобы добиться своего и в то же время не превратить отношения со своим парнем в театр военных действий. Конечно, не надо воспринимать все сказанное слишком серьезно - из любого правила есть исключения. В конце концов, может, эта статья - очередной тактический прием? :) Ведь писала-то ее девушка.

АЛЕКСАНДР '2POISONS' СИДОРОВСКИЙ (2POISONS@REAL.XAKEP.RU)

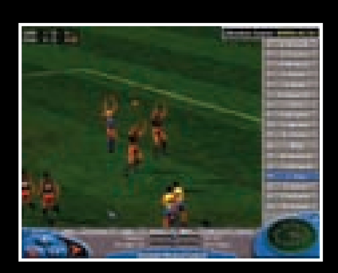




Урожденная Action Man 2: Destruction X
Жанр Аркадные гонки
Похожесть Action Man
Мать/отец Blitz Games/Infogrames Interactive
Требует P200(P2-300), 32(128), (3D)
Групповуха Обломись
Описуха Детские гоночки из серии Action Man (это которого сейчас в МакДаке в Хэппи Мил кладут). Носиться по трехмерным (кстати, симпатичным) уровням, отстреливать бандитов и нарушителей, спасать заложников, тушить пожары (???) - ну чем не мечта идиота? Боссы, разное оружие, погодные условия - ну просто must have какой-то... от 5 до 9.



Приговор СЛАБО

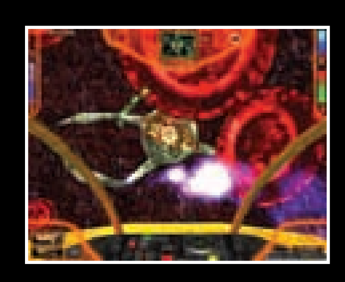


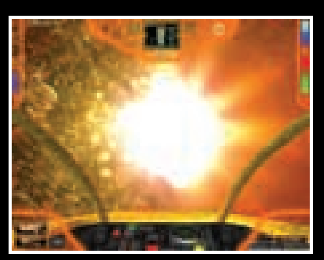


Урожденная Aussie Rules Coach
Жанр Спортивный менеджер
Похожесть футбольных менеджеров много, но такого...
Мать/отец Akaei
Требует P233(P2-300), 32(64), (3D)
Групповуха Обломись
Описуха Это менеджер австралийского футбола!!! А это, в свою очередь, такая зверюга, что мало не покажется: гремучая смесь футбола и регби. То есть таскать мяч в руках можно, но по воротам лучше бить ногой - очков больше получишь... Бр-р-р! Но игра не такая уж плохая: веселенькая, не напряжная. Примитивная, правда, ну да ладно - все равно ее никто всерьез воспринимать не будет.



Приговор СРЕДНЕ

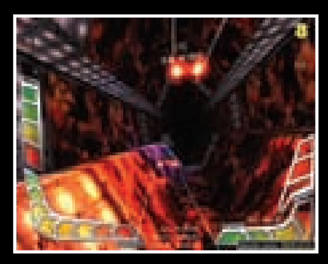




Урожденная Bacteria
Жанр action
Похожесть Sub-Culture, AMOK
Мать/отец FIN Arts/Net Games
Требует P2-300(P3-600), 64(128), 3D
Групповуха Обломись
Описуха Леталка с претензией на оригинальность. Носимся на микроскопического размера субмарине по кровеносным сосудам и другим полостям человеческого тела, отстреливаем злобных микробов, всякие там бактерии и вирусы, собираем бонусы, апгрейдим оружие, щиты... По сути - обычная аркадная леталка/плавалка. Но красивая, зараза.

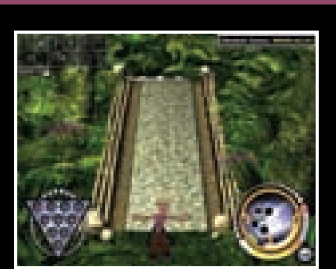
Приговор ХОРОШО

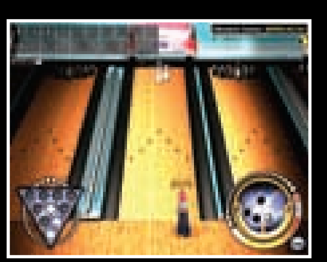




Урожденная Battlerace 3D
Жанр аркадные гонки
Похожесть Death Track, Descent
Мать/отец Soft Enterprises/Black Star
Требует P233(P2-300), 32(64), (3D)
Групповуха LAN, модем
Описуха Римейк одноименной игры (только без приставки 3D) образца 1996. За пять лет игра не претерпела никаких (!!!) сколько-нибудь серьезных изменений, разве что графику (ту же, 1996 года) под 3D ускорители оптимизировали. Все, больше ничего. Геймплей - банальные гонки на выживание на футуристических летательных аппаратах. Летаем по коридорам, как в Descent, отстреливаем конкурентов, как в Death Track. Старая добрая классика, понимаешь ли.

Приговор ЛАЖА



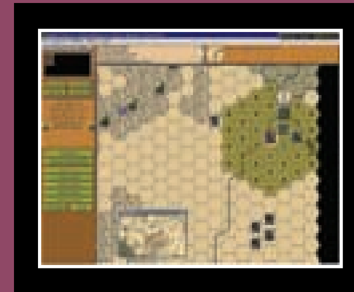
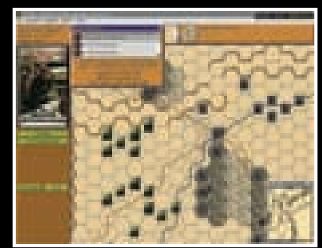


Урожденная Bowling Mania
Жанр bowling
Похожесть 3D Bowling USA
Мать/отец No.2 Games/eGames
Требует P200(P2-400), 32(64)
Групповуха Двое на одном компе
Описуха Дебильная поделка для детей, секретарш и американцев. Боулинг "с приколом". Играть можно на помойке, на кухне, на кладбище и т.д. Шар только один, игрок тоже. Никаких дополнительных условий, никакого инвентаря, даже настроек игры нормальных нет! Озвучка такая же аскетичная - три-четыре WAV'а и один MIDI или что-то типа этого. Редкостный отстой.

Приговор ЛАЖА

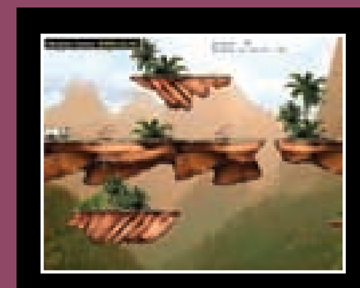
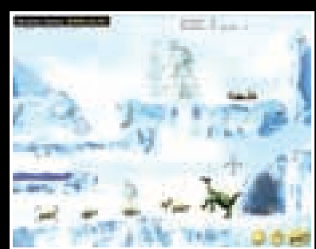
ЛАЖА → СЛАБО → СРЕДНЕ → ХОРОШО → РУЛЕЗ(З)!

Урожденная **Combat Command 2: Desert Rats**
Жанр wargame
Похожесть CC2: Danger Forward!
Мать/отец Boku Strategy Games/ Shrapnel Games
Требует P166(P200), 32(32)
Групповуха Hot-Seat, PBEM
Описуха Еще один варгейм из серии "Подавитесь своими ЖЫ-Форсами, у нас на дворе начало 90-х, ибо так стильно!" Действие происходит... угадай, где? Нет, не в Нормандии! Правильно, в Северной Африке - ведь каждый образованный школьник знает, что доблестная US-army при поддержке англичан и французов выиграла войну именно на этих двух фронтах. Про саму игру даже сказать нечего - обычное для этого жанра самоклонирование (предыдущая игра серии ничем не отличалась от нынешней, разве что действие разворачивалось... ага, правильно - в Нормандии).

Приговор **СРЕДНЕ**

Урожденная **Dinosaur'Us**
Жанр logic/arcade
Похожесть Lemmings
Мать/отец Digital Reality/Light & Shadow Production
Требует P166(P200), 32(32)
Групповуха split screen
Описуха Дело Леммингсов живет и побеждает! Смысл игры в следующем: у нас вылупляется куча динозавриков, и надо помочь им добраться от места появления на свет, до пещеры, где сидит мамаша. По дороги все кому не лень убивают их всеми доступными способами. Вот такая незамысловатая игруха. Lemmings были круче, наверное, во всех отношениях. Графика очень простенькая, двухмерная, уровни повторяются и, как следствие, Динозавры быстро надоедают.

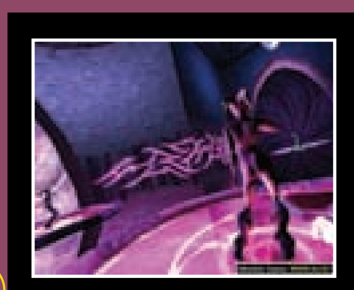
Приговор **СЛАБО**

Урожденная **Divided Ground**
Жанр wargame
Похожесть серия Battleground
Мать/отец Talonsoft
Требует P166(P2-266), 32(64)
Групповуха В ассортименте
Описуха Очередной обычно-добротный варгейм от Talonsoft в традициях Battlegrounds. На этот раз сражаться придется на арабо-израильском фронте с 1948-го по 73-й год. Ходы стали проще, теперь нет разделения на фазы, AI иногда способен впечатлить силой стратегического планирования, да и техника представлена довольно реалистично. Правда, все эти прелести смогут оценить только поклонники жанра - казуалов отпугнет условная графика и занудность геймплея.



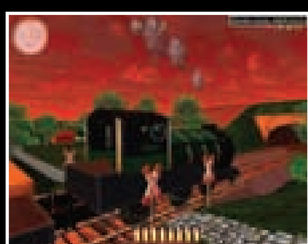

Приговор **СРЕДНЕ**

Урожденная **Dronez**
Жанр аркадный шутер
Похожесть Discs of Tron
Мать/отец Zetha Gamez
Требует P2-300(P3-700), 128(256), 3D
Групповуха Инет
Описуха Типичная аркада: прыгаешь по платформам, отстреливаешь шустрых, но непробиваемых врагов, подниимаешь бонусы... Один основной тип оружия (вспомнили MDK), невозможность нормально сохраняться, обалденно продвинутая, кричаще-яркая и местами очень красивая графика - все неотъемлемые атрибуты жанра при ней. Только вот кому это нужно?



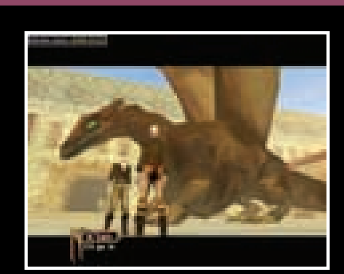
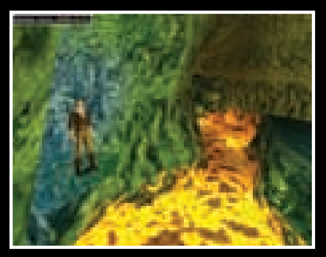

Приговор **СРЕДНЕ**

Урожденная **Get The Bunny**
Жанр аркадный шутер
Похожесть Moorhuhn
Мать/отец Soft Enterprises/Data Becker
Требует P2-300(P3-500), 64(128), (3D)
Групповуха Обломись
Описуха Смесь виртуального тира и охотничьего симулятора. Что-то типа бытовавшей во времена моего детства игрушки электронной "Ну, Погоди!". Только графика повеселее и арсенал оружия побольше. Отстреливаем кроликов, защищаем посевы морковки. Короче, безумно, ну просто бе-зумно затягивает... (хр-р-р...)

Приговор **СРЕДНЕ**

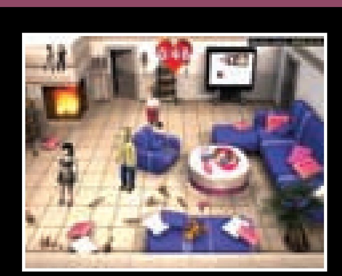
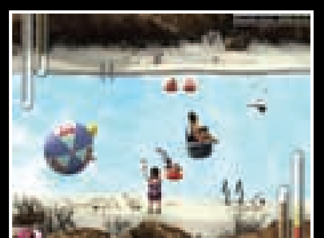


Урожденная **Dragon Riders: Chronicles of Pern**
Жанр adventure
Похожесть Drakan
Мать/отец Ubi Studios/Ubi Soft
Требует P2-300(P3-500), 32(128), 3D
Групповуха Обломись
Описуха Легковесная адвенчура на драконью тему. Есть бой (убогий), есть рост скиллов (кастрированный), есть куча суб-квестов (в стиле "подай-принеси"), есть качественно озвученные диалоги (очень длинные и скучные), есть симпатичная графика и красивые мультики (повторяющиеся при каждом перелете в другой локейшн и осточертевающие уже на третьем просмотре) - одним словом, есть многое, но все это както криво сделано. Правда, несмотря на это, игра оставляет в целом положительные впечатления. Типичная "купил-заценил-поставил-на-полку-забыл".

Приговор **СРЕДНЕ**



Урожденная **Girlscamp**
Жанр TV show
Похожесть Big Brother
Мать/отец Novatrix/Shoebox Interactive
Требует P2-300(P3-500), 64(128), (3D)
Групповуха Обломись
Описуха До чего доходят люди в припадках творческого кризиса! Эта игра - симулятор телевизионного шоу, в котором зрители наблюдают в реальном времени за подопытными девушками, живущими на специально отведенной вилле на Канарах. Зачем? Ну просто так. Зачем в Инете ставят "живые камеры"? Вот и это то же самое. Периодически одна из участниц покидает игру либо потому что за это проголосовали телезрители, либо по другим причинам (способов "выбить" девушку много). В конце остается только одна - она и получает солидный приз за выигрыш. Вот все это хозяйство и симулируется в игре Girlscamp. Помесь The Sims и передачи для домохозяек.

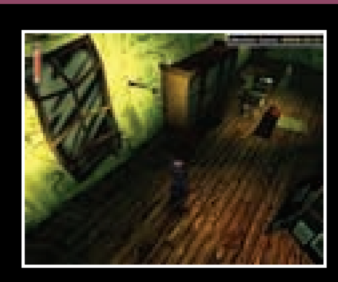
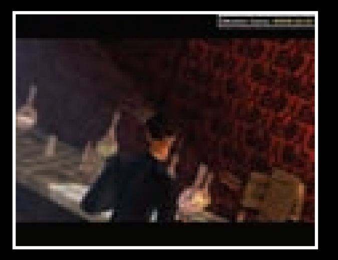
Приговор **ЛАЖА**



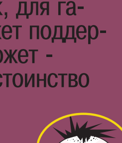


Урожденная **Green Berets (powered by Myth II)**
Жанр трехмерная стратегия
Похожесть Myth II: Soulblighter
Мать/отец Take 2 Interactive
Требует P200(P2-300), 32(64), (3D), Myth II CD
Групповуха В ассортименте
Описуха По сути это Total Conversion старого доброго Myth II. Только вместо гномов и лучников - саперы и снайперы, а вместо всякой тролле-орко-гоблинской нечисти - бойцы вьетконговской армии освобождения. Геймплей прост как интерфейс тетриса - пять-шесть бравых десантников бродят по насквозь протрехмеренной карте и превращают роты и батальоны врагов Америки в тонны мясного вторсырья. Графика та же, эффекты те же, игровой процесс тот же. Myth II 98-го года с перекрашенными текстурами. Вот такой "Миф-Универсал"

Приговор **СЛАБО**

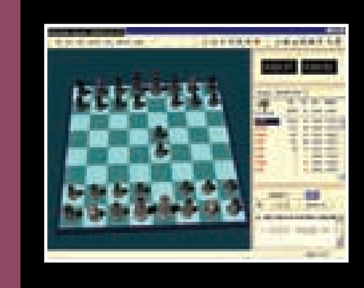
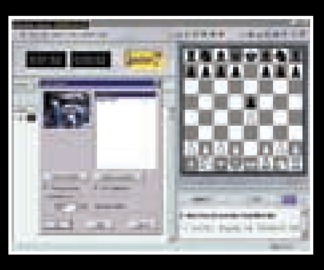
Урожденная **Jekyll & Hyde**
Жанр TPS/квест
Похожесть American McGee's Alice
Мать/отец In Utero/Cryo Interactive
Требует P2-400(P3-600), 64(128), 3D
Групповуха Обломись
Описуха Жестоко испохабленная McGee's Alice. Такая же атмосфера плавного, но неизбежного съезда крыши, вот только реализовано все на порядок хуже. Скучная коричнево-зеленая палитра, кривые и бедные полигоны. Играется так: бегаем, прыгаем, скачем с платформы на платформу, бац! - упали. Начинаем с последнего чекпоинта - сохраняться где хочешь тут нельзя. Еще осталось желание играть? Оно отпадет, когда ты увидишь жутко неудобную камеру, которая так и норовит показать самый неудачный ракурс. А квест? Так, для галочки, чтобы сюжет поддержать... Кстати, сюжет - единственное достоинство этой игры.



Приговор **СЛАБО**

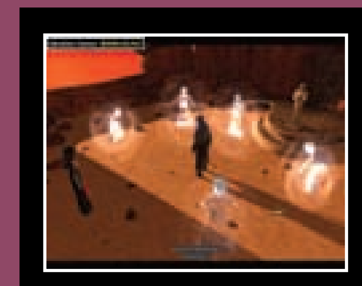
ЛАЖА → СЛАБО → СРЕДНЕ → ХОРОШО → РУЛЕЗ(З)!

Урожденная **Junior 7.0**
Жанр шахматы
Похожесть Fritz 6, Nimzo 8
Мать/отец Chessbase
Требует P233(P2-266), 32(64)
Групповуха Обломись
Описуха Не выдающийся ничем шахматный сим с достаточно именитой родословной. Заточен явно не под новичков - никаких тебе интерактивных курсов обучения, если не умеешь играть, читай рулесы с компакта. Зато имеются гора настроек и туча опций. Подойдет тому, кто имеет некоторый опыт в этом жанре. Играет Junior очень грамотно, оформлен аскетично, но не скупо - как раз так, как и должен выглядеть chess sim. В общем, такой добротный середнячок получился.

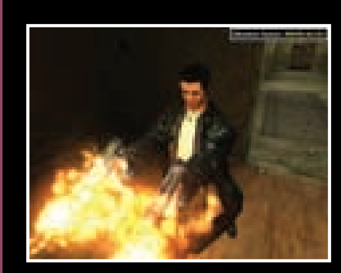
Приговор **СРЕДНЕ**

Урожденная **Legend II: Secrets of Alamut**
Жанр Квест
Похожесть The Legend of The Prophet And The Assassin
Мать/отец Arxel Tribe/Cryo Interactive
Требует P233(P2-300), 32(64)
Групповуха Обломись
Описуха Вторая часть сериала Пророк и Убийца не сильно отличается от первой. Движок остался прежним, графика тоже, хотя ее и так менять не стоило. Правда, загадки стали логичнее и приятнее. Самая сильная сторона игры - погружение в атмосферу, созданную сюжетом (пересказывать не буду - места нет, да и кайф не хочу обламывать). Самая слабая - стремление разработчиков строго следовать сюжету Пабло Коэльо, иногда даже в ущерб играбельности.



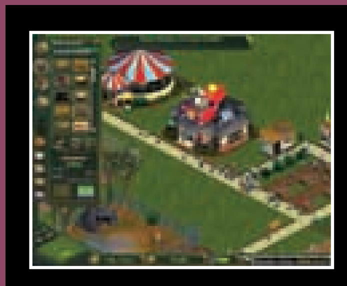
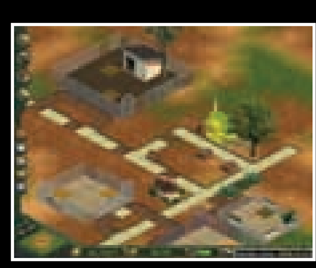

Приговор **ХОРОШО**

Урожденная **Max Payne**
Жанр 3D TPS
Похожесть Oni, Heretic 2
Мать/отец Remedy Entertainment/ G.O.D. Games/Take 2
Требует P2-450(Athlon-1000), 96(256), 3D
Групповуха Обломись
Описуха Мы это долго ждали. И дождались. Лично я теперь под это дело буду специально комп апгрейдить. Такой атмосферы еще не было нигде. Перестрелки в лучших традициях Матрицы и фильмов Джона Ву, умопомрачительная физика, идеальная графика, абсолютная интерактивность мира. Я, часом, не загибаю? Нет, не загибаю - пожалуй, это одна из лучших, если не лучшая игра года.



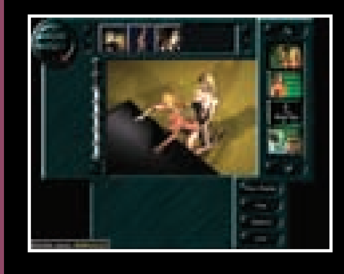
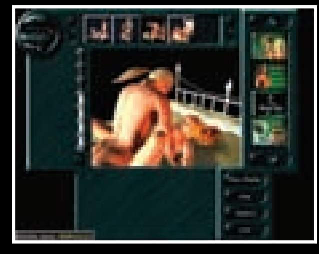

Приговор **РУЛЕЗЗЗ!**

Урожденная **Zoo Tycoon**
Жанр tycoon
Похожесть см. жанр
Мать/отец Blue Fang Games/Microsoft
Требует P233(P2-300), 32(64)
Групповуха Обломись
Описуха Ну, е-мое, еще один обычный тайкун! Давайте я перечислю, что нужно делать в этой игре... Нет, лучше не буду: открой любой из номеров Х, там в Зале Суда почти наверняка будет такое же описание. Графика традиционно двухмерная, мультяшная, но не раздражает. Реализация качественная, все-таки Майкрософт издает. Мне эта игра больше всего напомнила Roller Coaster Tycoon - очень похоже, только там аттракционы, а тут зоопарк. Игра неплохая, но только для коллекционеров.

Приговор **РУЛЕЗЗЗ!**

Урожденная **Never Ending Fantasies Machine**
Жанр виртуальный секс
Похожесть Virtual Sex
Мать/отец Exo Studios
Требует P2-300(P3-500), 32(128)
Групповуха Обломись
Описуха Это что-то типа 3D-порно плеера. Выбираешь трехмерный мультик и вперед - одной рукой выбираешь наиболее удобные ракурсы камеры и слегка вмешиваешься в происходящие (ну там, если шлепнуть кого-нибудь хочешь или чтобы они позу поменяли), вторая рука остается свободной для любых других занятий ;). Новые мультики, или, как их называют авторы, фантазии можно скачивать с сайта разработчиков. Даже редактор поставляется, чтобы самому такие шедевры трехмерного искусства ваять.

Приговор **НА ЛЮБИТЕЛЯ**



"У.О." — не обязательно "умственно отсталый"

Подключись к Ultima Online бесплатно!

FaraoN ака Петухов Семён (FaraoN_Semen@rambler.ru)

Примечание: редакция выражает робкую надежду на то, что ни один из здравомыслящих читателей не будет пробовать повторить действия, описанные в статье. По крайней мере, за проваленные сессии, разрушенные семьи и папины зарплаты, потраченные на оплату Интернета, редакция Х и автор статьи ответственности не несет.

Я пишу из глубин Интернета, из сказочных миров, откуда нет возврата, из игры, в которую однажды случайно попал. Я давно уже живу в ином мире, в мире-ловушке под названием Ultima Online. А ведь на самом деле я еще жив, сижу где-то на стуле перед монитором, только я этого уже не могу осознать, потому что в моей реальной жизни я бегаю по миру Британии, убивая монстров и драконов, колдую и прыгаю в телепортаторы, пересекаю сотни километров за доли секунды. Дел много, времени нет. Бывает, что убивают и меня, но я уже не боюсь смерти, я знаю, что рано или поздно найду крест и воскресну, а значит, снова буду убивать, и снова будут убивать меня! Это ловушка, похожая на реальный мир - мир, где ты обретешь десятки новых надежных друзей и сотни врагов, которые убьют тебя ради наживы, мир, где тебя могут спасти или предать люди, от которых ты этого не ожидал.

А я ведь помню, как все начиналось: я искал нормальную многопользовательскую игру около года или двух лет назад (теперь я уже потерялся во времени), и мне рассказали про Ultima Online. Я пошел и купил ее (как часто я думаю, что бы со мной было, если б мне про нее не рассказали: я мог бы отдохнуть на море или стать кинозвездой, или купить себе новый компьютер), после этого я последовал всем инструкциям и начал играть. Сначала игра завлекла не так сильно, и я проводил в ней не больше часа в день, но очень скоро стал играть все больше и больше, вскоре мне уже понадобился анлим, а родственники забыли о такой прелести, как телефон. Вот тогда-то все и началось.

Ниже я опишу действия, которые ты ни в коем случае не должен делать, иначе ты станешь одним из тысяч таких как я, (не думай что я один такой; куча народу оккупировала мир Британии, и те, у кого нет дома компа, терроризируют родителей на инвестиции, чтобы десяток-другой часов просидеть в клубе).

Где купить игру (хотя лучше этого не делать!)

Диск с игрой можно достать на рынке или в магазине. Сразу говорю, не ищи русскую версию - ее нет. Всего бывает две версии ултимы: UO TA2 и просто UO, но в игре они практически ничем не отличаются. А вот патчи для них нужны разные, поэтому при покупке уточняй у продавца версию игры.

Где начать игру (если ты все-таки купил диск с игрой, выкини свой комп в окно)

По идее мы с тобой должны играть на буржуйском серваке и платить за это деньги. Но наши

Наши люди о себе позаботились (да и не только наши) и придумали различные эмуляторы сервера - шарды, так что теперь можно не просто играть, общаясь на русском (и даже писать кириллицей), но и делать это абсолютно бесплатно, то есть на халяву!

люди о себе позаботились (да и не только наши) и придумали различные эмуляторы сервера - шарды, так что теперь можно не просто играть, общаясь на русском (и даже писать кириллицей), но и делать это абсолютно бесплатно, то есть на халяву! Среди русских шардов есть много хороших старых шардов, с большим количеством игроков, и есть много новых шардов, на которых народу поменьше. У обоих есть свои преимущества: на новых шардах нет очень сильных опытных игроков, которые легко побеждают новичков, и все игроки начинают игру на равных, зависят друг от друга (у кого-то высокий параметр горного дела, у кого-то - плотника, у кого-то - лесоруба, у кого-то кузнечное дело и т.д.). А на старых шардах уже есть мощные игроки, которые могут помочь новичкам, а могут и, наоборот, подзаработать на их неопытности и слабости, что, увы, бывает часто. На старых, известных шардах играет много народу, что дает возможность выбирать, с кем общаться, а с кем воевать. Так что сам выбирай, на каком шарде тебе играть, но для начала попробуй поиграть на нескольких разных шардах перед тем как выбрать место для своего постоянного пребывания. Вот небольшой список подходящих шардов:

http://ultima.pp.ru - очень хороший и интересный отечественный шард Ethereal Portal, с заботливой и внимательной администрацией.

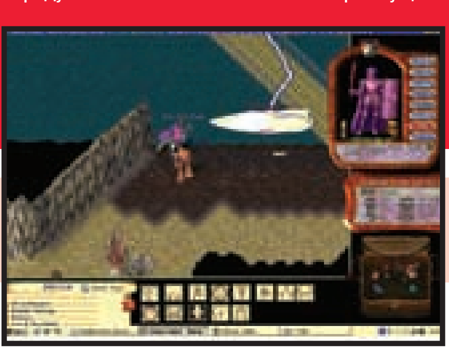
http://ultima.tagan-rog.ru - лучший новый сервер. Для тех, кто хотел бы играть на новом шарде с небольшим количеством крутых игроков.

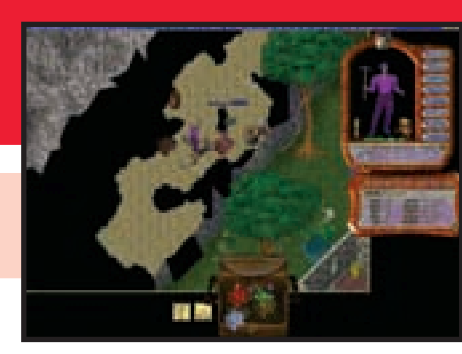
http://ultima.com.ru - официальный сайт Оскома (шарда CSD UO).

http://www.novusopiate.com - еще один хороший и старый игровой сервер Ultima Online, но Ethereal Portal, по-моему, интереснее.

http://www.zuluhotel.com/uo - хороший буржуйский УО шард, основан на кодовой базе POL (ultimate scripting), которую доводили до ума больше года.

Это не полный список, но здесь представлены все лучшие сервера для игры в эту заразу.





Как начать игру (если жить надоело в реале)

На сайте шарда написано обо всем необходимом для этого. В основном есть несколько основных правил: тебе нужно скачать файлы из соответствующего раздела и переписать их в основную директорию UO, только все подряд не качай, я бы советовал ограничиться только файлом login.cfg и EXEшником. После этого тебе нужно перейти в раздел аккаунт и завести там на себя учетную запись, но на некоторых серверах регистрация реализована по-другому, например, учетная запись создается при первом коннекте с таким логином или нужно высылать просьбу о создании аккаунта. Теперь нужно создавать персонажа. Первый этап создания персонажа - выбор профессии. Сначала тебе будет предложено выбрать тип будущего героя: Adventurer, Merchant или Advanced. Последний вариант рассчитан на опытных игроков, так что его выбирать пока не стоит.

Выбор между первым и вторым типами зависит от стиля игры, который ты предпочитаешь. Если тебе по приколу всякие дальние странствия, сражения с чудовищами и другие героические занятия, выбирай Приключенца. А если больше нравится общение, политика, торговля или просто мирная жизнь, тебе больше подойдет роль Торговца.

Затем тебе будет предложено уточнить область деятельности своего персонажа. Например, Приключенец может быть Воином, Лучником или Магом. Каждая область деятельности, в свою очередь, включает в себя несколько профессий, подробное описание каждой из которых появляется в текстовом поле.

Выбор профессии приводит к изменению некоторых качеств и навыков твоего героя, однако в целом все вновь созданные персонажи обладают равными возможностями.

Как зарабатывать деньги в UO

Поначалу будет очень сложно зарабатывать деньги, особенно на новых шардах, но на старых есть пара безотказных способов.

При создании персонажа выбери одним из своих параметров Mining (Горное дело) и поставь силу на максимум, а в самой игре найди какую-нибудь пещеру, накопай там побольше руды и переплавь ее. Полученный Iron ingot можно продать по 10gp за шт. какому-нибудь игроку.

Будь осторожен со своим паролем: если ты играешь в клубе, то, когда отходишь за пивом, делай дисконнект, потому что сменить пароль и е-майл - дело трех секунд, а по правилам любого шарда восстановить аккаунт нельзя.

Второй способ: примерно такая же схема, только при создании персонажа возьми ему скилл лесоруба и руби логи (бревна), их можно продать по 20gp за шт. Этот способ даже лучше, т.к. если тебя вдруг сошлют в Сибирь на каторгу, тебе будет легче на лесоповале.

Под конец пара технических вопросов. Например, вопрос безопасности. В Интернете всегда найдутся читеры, которым лень прокачивать своего персонажа, и они попросту воруют чужих. Так что будь осторожен со своим паролем: если ты играешь в клубе, то, когда отходишь за пивом, делай дисконнект, потому что сменить пароль и е-майл - дело трех секунд, а по правилам любого шарда восстановить аккаунт нельзя. Еще хочу предупредить о том, что мало кому понравится, если к нему будут приставать с дурацкими вопросами, так что помни золотое правило RTFM: почитай сначала раздел для новичков!

А вообще, мы тебя вначале предупреждали - сперва дважды подумай, нужно ли тебе все это. Потому что подсесть на UO вполне реально, а деньги за Инет придется платить совсем не в ультимовских gp.

П.С. Моя особая благодарность за помощь при создании данной статьи Counselor Bers'у и Miledi, да и всему Ethereal Portal за ту атмосферу сказки, которую они создали на своем шарде.

Ломка

KodeMaster (cranyoblast@real.xakep.ru)

Коды

Max Payne

Запусти игру с параметром -developer (ну что-то типа C:\maxpayne\maxpayne.exe -developer) и ты сможешь вызывать консоль по клавише F12. В эту самую консоль и вбивай коды.

coder - Все читы в одном флаконе. Теперь ты бессмертный чувак, упакованный всеми стволами и бесконечным боезапасом. Если сможешь проиграть, получишь от нас приз "Ламер Месяца".
god - Неуязвимость обычная, одна штука.
mortal - На фиг неуязвимость. Hurt me, baby!
getallweapons - Ты ограбил оружейный магазин...
getinfiniteammo - В придачу со складом боеприпасов!
noclip - Никаких клипов по телеку! В смысле - через стены ходить можно...
noclip_off - Ура! Снова клипы по ящику! В смысле - опять нельзя...
getbullettime - А пули летят, пу-у-ули-и-и! Врубаем Bullet Time.
showfps - Насладись мощью своего свежекупленного третьего пня! Зацени frame rate.
c_addhealth (100) - Ты сожрал 100 пачек детского панадола (по одной пачке на каждый хит-поинт).
jump10 - Прыгучесть, как у австралийских кузнечиков (попробуй подставить значения 20 или 30, чтобы почувствовать себя Бубкой).
SetWoundedState - Без меня тебе, любимый мой, лететь с одним крылом! Ходишь, как будто из реанимации сбежал.
SetNormalState - Опять все в норме. Походка, как у часовых возле мавзолея.

Введи эти коды, чтобы получить соответствующие предметы:

GetBaseballbat
GetBeretta
GetBerettaDual или GetDualBeretta
GetDesertEagle
GetSawedShotgun
GetPumpShotgun
GetJackhammer
GetIngram
GetIngramDual или GetDualIngram
GetMP5
GetColtCommando
GetGrenade
GetM79
GetSniper
GetHealth
GetPainkillers

Conflict Zone

Во время игры клавишей вызываешь chat window (клавиша C), жмякаешь BACKSPACE и вводишь коды.

WIN - Поздравляем! Миссия закончена успешно!
MY TAYLOR IS RICH - 20000 очков и 100% популярности. Можно баллотироваться в президенты.
REPLAY ALL MISSIONS - Все миссии становятся доступными как представительницы древнейшей профессии.

FIFA 2001

В главном меню набери:

Gimmethemoney - деньги на бочку!
Playersmaybe - бесплатные CD-плееры, DVD-плееры, MP3-плееры, а также football-плееры.
Bigheads - а теперь у этих футбол-плееров отрастают большие... нет, нет - всего-навсего большие головы.
Playersarelocked - игроки команды соперника стоят как парализованные.
Lightsout - если вырубить свет, футболисты будут светиться, как будто они - сборная Чернобыля.
Dizzy - с неба на футбольное поле сыплются инопланетяне.

Startopia

Во время игры задави F11 и набирай RSHIFT. Ты, по идее, должен увидеть какое-либо случайное сообщение - это значит, что читы активированы. Теперь тебе нужно активировать каждый конкретный чит (вот идиотизм!) для того чтобы потом его юзать с правым SHIFT'ом. Делается это так: зажимаешь F11 и вводишь RSHIFTSPEEDUP. Теперь, если ты с правым шифтом нажмешь " > ", скорость игры увеличится (чем дольше давишь, тем шустрее игра). Если вместо этой пимбы юзать знак "меньше" (это вот такой < отморозок над буквой "Б"), то игра будет (никогда не догадаешься) замедляться! Клавиша "L" возвращает игру в нормальный режим.
А вот еще прикольный код: давишь F11 и набираешь CLIVEROOLZ. Опа! Теперь игра эмулирует Spectrum (в смысле переключается в его стандартное разрешение 256x192). Набираешь то же самое еще раз - получаешь навороченный Spectrum :) (то есть можешь выбрать любое его разрешение). Набираешь в третий раз - опять старая PC'шная зараза (back to normal то бишь :).

Хексы

Technomage

В директории с игрой ищешь папку SAVES. В ней по идее должны лежать файлы с именами типа tmn_01.tsg, tmn_02.tsg и так до 10. Это твои сохраненки (сюрприз, сюрприз!). Открываешь свою любимую сейв-гейму хекс-редактором и начинаешь все конкретно хекс-редактировать.

Чтобы получить skill items (типа fireball, earthquake и т.д.), пропиши значение 01 по следующим адресам:

4b18,4b1c
4b20,4b24,4b28,4b2c
4b30,4b34,4b38,4b3c
4b40,4b44,4b48,4b4c
4b50,4b54,4b58,4b5c
4b60,4b64,4b68,4b6c
4b70,4b74,4b78,4b7c

Если где-то уже стоит не нулевое значение, менять, разумеется, ничего не надо.

Теперь попробуем напихать в инвентори всяких полезных шмоток. За 27 инвентарных слотов отвечают адреса с 4f14 до 4f49, по 2 байта на рыло. Если слот пустой, значения будут такими: ff ff, но ведь нам пустые слоты не нужны, верно? Так что первым значением мы подставим код нужного предмета, а второе обозначим как 00. Только этого мало. Чтобы предмет появился в инвентори, нужно еще указать количество этих самых предметов. Ниже приведен список нужных кодов и адреса, куда тебе придется вставлять желаемое количество штук (даны в скобках).

1b - arrows (4b80 - ff для неограниченного боекомплекта)
1c - fire arrows (4b84 - ff для неограниченного боекомплекта)
1d - water arrows (4b88 - ff для неограниченного боекомплекта)
1e - small healing potion (4b8c)
1f - large healing potion (4b90)
20 - small combined potion (4b94)
21 - large combined potion (4b98)
22 - small mana potion (4b9c)
23 - large mana potion (4ba0)
24 - anti-venom herb (4ba4)
25 - anti-venom potion (4ba8)
26 - magic cube (strength) (4bac)
27 - magic cube (intelligence) (4bb0)
28 - magic cube (constitution) (4bb4)
29 - magic cube (mystic) (4bb8)
2a - copper key (4bbc)
2b - silver key (4bc0)
2c - gold key (4bc4)
2d - steel key (4bc8)
2f - torch (4bd0)
31 - compass (N/A)
32 - chalk (4bdc)

Dreamertown:

39 - a rose (4bf8)
3a - Mrs. Sengarn's books (4bfc)
3b - a balloon, somewhat deflated (4c00)
3c - shade fern (4c04)
3d - bread and butter (4c08)
3e - Master Bacchus' best booze (4c0c)
3f - sleeping draught (4c10)

Steamertown:
40 - crowbar (4c14)
41 - lump of zantium (4c18)
42 - kitten (4c1c)
43 - cork (4c20)
44 - castor oil (4c24)
45 - empty stew plate (4c28)
46 - stew (4c2c)
47 - stew with castor oil (4c30)
48 - dynamite (4c34)
49 - control wheel (4c38)
4a - oil can (4c3c)

The Hive:
4b - black module (4c40)
4c - blue module (4c44)
4d - green module (4c48)
4e - red module (4c4c)

Fairy Forest:
4f - silverweed (4c50)
50 - blue ice flower (4c54)
51 - red sunflower (4c58)
52 - dark green flower (4c5c)
53 - light green spring flower (4c60)
54 - honeycomb (4c64 - складывается со значением другого honeycomb)
55 - branch from an old oak (4c68)
56 - Horpach's magic wand (4c6c)
57 - good luck potion (4c70)
58 - yellow crystal (4c74)
59 - honeycomb (4c78)
5a - empty bucket (4c7c)
5b - bucket of fresh water (4c80)
5c - captured bee (4c84)
5d - fish seal (4c88)
5e - horse seal (4c8c)
5f - bird seal (4c90)
60 - shrinking potion (4c94)
61 - harp strings (4c98)
62 - knife (4c9c)
63 - silk thread (4ca0)
64 - bee sting (4ca4)
65 - fairy gold (4ca8)
66 - bee basket (4cac)
67 - wooden mask (pass) (4cb0)
68 - ray glass (4cb4)
69 - moonbeams in a ray glass (4cb8)
6a - antidote potion (4cbc)
6b - antidote potion blessed by a royal smile (4cc0)
6c - tuning fork (4cc4)
6d - honey glass (for catching bees) (4cc8)
6e - gear wheel (4ccc)

Canyon:
6f - red eye stone (4cd0)
70 - green eye stone (4cd4)
71 - blue eye stone (4cd8)
72 - yellow eye stone (4cdc)
74 - red lens (4ce4)
75 - green lens (4ce8)
76 - blue lens (4cec)
77 - Cahoch-Ran's horn (4cf0)
78 - lever (4cf4)
79 - old spectacles (4cf8)

Tower:
7a - black pearl (4d00)
7b - belladonna (4d04)
7c - empty urn (4d08)
7d - urn filled with ashes (4d0c)
7e - book on ghost conjuring (4d10)

Volcano:
80 - blue iron ball (4d14)
81 - bucket (4d18)
82 - lump of metal (4d1c)
83 - Ruisorne's voting coin (4d20)
84 - gambler's voting coin (4d24)
85 - Cistorne's voting coin (4d28)
86 - the evidence (4d2c)
87 - shovel (4d30)
88 - crystal (4d34)
89 - stardust (4d38)
8a - geode (4d3c)
8b - book (4d40)
8c - amulet (4d44)
8d - crystal (4d48)
8e - dragon's tooth (4d4c)
8f - egg from the hive (4d50)
90 - goblet of mead (4d54)
91 - nut (4d58)
92 - mushroom (4d5c)
93 - ring (4d60)
94 - skull (4d64)
95 - shard of mana crystal (4d68)

Ruins:
96 - fish (4d6c)
97 - berries (4d70)
98 - black keystone (4d74)
99 - white keystone (4d78)
9a - red keystone (4d7c)
9b - blue keystone (4d80)
9c - green keystone (4d84)
9d - yellow keystone (4d88)
9e - energy pearl (4d8c)
9f - seal of mysticism (4d90)
a0 - seal of combat (4d94)
a1 - seal of defence (4d98)
a2 - seal of magic (4d9c)

Учти, что многие предметы из этого списка будут глючить, если ты попытаешься получить их не на том уровне, для которого они "предназначены".

Золото можно получить здесь: 4be0-2. Максимальное количество ($999999) - 3f 42 0f.
Скиллы лежат тут:
73ad - Strength (STR); Max 28 hex
73ae - Intelligence (INT); Max 28 hex
73af - Constitution (CON); Max 28 hex
73b0 - Mystical (MYS); Max 28 hex

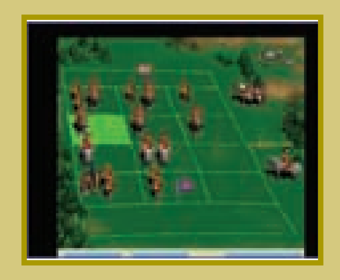
WWW – Развлекухи

Александр '2poisonS' Сидоровский (2poisonS@xakep.ru)

Conquest of The New World

http://games.zone.ru/games/battle.html

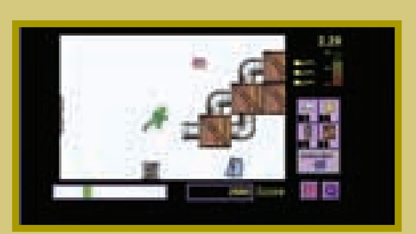
Когда-то давным-давно так называлась одна походовая стратегия про завоевание Америки. Лично мне в этой игре больше всего нравилось, как там реализованы бои между колонистами разных стран или коренными жителями. Сама стратегия была так себе, а вот бои - просто улет. Хорошо, что там был отдельный режим игры, когда можно было выключить на фиг все развитие, набрать себе армию и... Эх, были деньки! Хотя почему - были? Пусть диск с Conquest of The New World потерт, поцарапан и потерян (а даже если бы и стоял сейчас на полке на расстоянии вытянутой руки - все равно ничто на свете не заставило бы меня тратить время на это старье), окунуться в любимые когда-то сражения колонистов с индейцами можно прямо в Инете, и даже ничего не сгружая себе на винт. Жаль, армию набирать самому не дают, приходится воевать всегда одним и тем же отрядом.



Get The Pants

http://games.zone.ru/games/get.html

Еще одна развлекуха из неплохого сборника онлайн-игр games.zone.ru. "Поймай штаны" называется. В описании тебе предложат ознакомиться с душераздирающей историей про школьника, которого преследовал сон о том, как он приходит в школу абсолютно голый и убегает по коридорам от директора под дружный гогот друзей и подруг. Надо полагать, под воздействием постоянного невроза у бедняги окончательно поехала крыша, и в один прекрасный день, когда он проснулся утром и, как обычно, протянул руку за любимыми джинсами - их не оказалось на месте. Предательские штаны убегали от него не хуже, чем всякие самовары и сковородки из детского стишка про Федорино горе. Не ожидая от своего больного сознания такой подставы, наш герой пустился вслед за глюком в виде штанов. Разумеется, в чем мать родила. И вот этот порнофильм с элементами психоделического action и лег в основу сюжета игры Get The Pants. Основная задача игрока - догнать непослушный предмет одежды, впрыгнуть в него и успеть до звонка на первый урок в школу. Обычные трудовые будни американского подростка.



Kangoo vs Kangoo

http://www.newgrounds.com/portal/frames.php?id=8705

Настоящий мултиплеерный файтинг! Два жирных кенгуру на маленьком ринге выясняют, кто же из них кенгурее всех кенгурых, потому что только один выйдет победителем в этой схватке. Три удара: рукой, ногой и - хит сезона - ногой с разворота, живой соперник на другом конце клавиатуры и море незамутненного кенгуристского action - вот чем, по мнению Х, нужно скрашивать рутинные будни в унылом офисе. Кенгурятина rulezz forever!!!

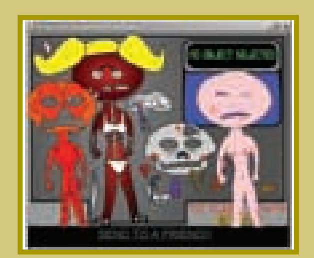
Нет, если серьезно, мне уже слегка поднадоели эти одинаковые мочилова со всякими самураями-каратистами-кикбоксерами-спецназовцами и непременными фонтанами крови, которая заливает весь монитор, разве что на клаву не капает. Расчлененка - это, конечно, хорошо, но быстро надоедает. То ли дело неповоротливые жирные кенгуриные туши: удар с ноги выглядит как попытка перекормленного инвалида забраться на унитаз, динамика боя напоминает уставших на смерть борцов сумо, которые отдыхают в объятьях друг друга, и никакой запарки с управлением. Можно выписывать в качестве транквилизатора.



Claris Autopsy

www.newgrounds.com/portal/frames.php?id=5394

Тебе когда-нибудь приходилось проводить вскрытие? Нет? Много потерял, приятель, - это такое увлекательное занятие! Особенно если препарируемый сабжект - девочка-подросток, погибшая при загадочных обстоятельствах. Твоя задача - внимательно осмотреть тело снаружи и изнутри и установить причину смерти. Когда будешь по очереди вытаскивать желудок, почки, печень, кишки и прочие девичьи прелести, будь очень внимателен: причина смерти может обнаружиться где угодно. Хотя... пациент какой-то странный попался, привезли на вскрытие, а сердце вроде бьется... Ну, нам, медикам, все равно - сказали резать, значит будем резать. И живая она там или нет - вскрытие покажет.



M.J.Ash / www.xknows.bos.ru / m.j.ash@real.xakep.ru

Сентябрь. Время покупать своему электронному другу новые железки и модернизировать ПО. Скромно предполагая, что в выборе правильных программ кое-кто из читателей "Х" ориентируется на материалы этой рубрики, я решил продолжить тему "Необходимых вещей", начатую в мартовском номере (http://magazine1.xakep.ru/xa/027/092/1.asp). Надеюсь, что и эта порция моего любимого софта придется тебе, коллега, по вкусу. :)

CNET CatchUp v 1.3

Windows 9x/Me/NT/2k
Size: 772 Kb
Freeware
http://catchup.cnet.com

CatchUP - бесплатная Internet-служба, которая автоматически определяет, какие программы на твоем компьютере нуждаются в обновлении. Для работы с ней тебе потребуется предварительно скачать и установить небольшую утилиту-клиента. Управляется эта утилита через браузер. На сайте службы ты просто кликаешь по ссылке "Software Updates", на следующей страничке давишь кнопку с надписью "Launch CatchUP", и CatchUp-клиент запускается сам. Он сканирует твои жесткие диски в поисках знакомых ему исполняемых файлов и компонентов приложений, консультируется с обширнейшей базой данных CNet.com, после чего показывает тебе веб-страничку со ссылками на файлы обновлений! Вся операция занимает несколько минут.

Отдельно стоит отметить, что на сайте CatchUP рядом с "Software Updates" располагается ссылка на "Security Fixes". Не пропусти ее! Ведь при посещении этого раздела твой компьютер подвергнется повторному сканированию, в ходе которого выяснится, какие у него имеются дыры в системе безопасности и какими патчами их можно залатать.

TaskInfo2000 v 3.0.10

Windows 9x/Me/NT/2k
Size: 631 Kb
Shareware
http://www.iarsn.com

Отличная программа, которая сочетает в себе свойства менеджера задач и системного информатора. С ее помощью всегда можно точно узнать, какие процессы выполняются на твоей машине, откуда они стартовали и какие файлы используют. Кроме того, TaskInfo2000 наглядно показывает, сколько какая программа занимает памяти и процессорного времени. Ясное дело, что при этом любой процесс, чьи аппетиты или само существование противоречат твоим интересам, можно убить или, по крайней мере, изменить приоритет его выполнения. Под Windows 98 иметь под рукой прогу вроде этой жизненно необходимо, поскольку стандартный менеджер задач в этой операционке на редкость примитивен. Им зависшее приложение замучаешься закрывать, не то что трояна отлавливать! Впрочем, даже если ты работаешь под NT/2k, эта прога должна показаться тебе интересной, поскольку она, кроме всего прочего, сообщает юзеру массу детальной информации об операционной системе, процессоре, свободной памяти, использовании кэша, своп-файла и т.д.

GoBack v 3.0 Deluxe

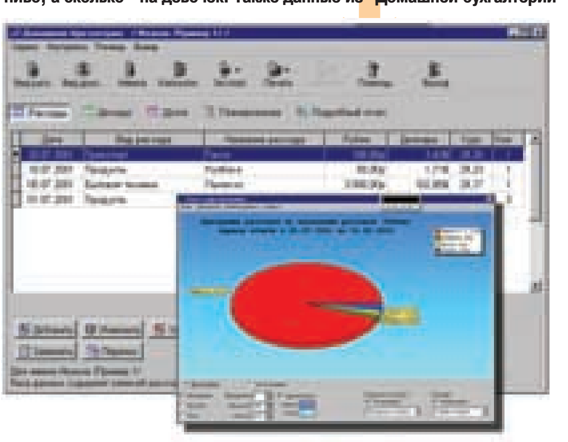
Windows 9x/Me/NT/2k
Size: 8002 Kb
Shareware
http://www.goback.com

Еще полгода назад я активно рекламировал программу SecondChance как надежное средство от компьютерных вирусов, системных глюков и ошибок пользователя. Но, по закону подлости, не успел мартовский номер Х с моим описанием прелестей "Второго Шанса" появиться в продаже, как компания PowerQuest сообщила, что жизненный цикл этой замечательной проги, к сожалению, подошел к концу, и она вынуждена изъять ее из оборота! Естественно, нашлись люди, которые тут же предположили, что я имею самое непосредственное отношение к этому свинству, и поспешили излить на меня свое негодование в письмах :). Впрочем, я отвлекся. Вследствие безвременной кончины "Второго Шанса" последней надеждой продвинутого юзера на безоблачную жизнь стал его единственный конкурент - программа GoBack. К счастью, разработку этой проги никто (вроде… тьфу, тьфу, тьфу! :) сворачивать не собирается. Наоборот - не так давно появилась GoBack v 3.0 Deluxe, которая (в отличие от ныне дохлой SecondChance) может работать не только под 98-ми Виндами, но и под NT/2k!!! При этом функционирует GoBack точно так же, как и SecondChance, т.е. постоянно протоколирует все дисковые операции и сохраняет в специально отведенной области на жестком диске всю затираемую инфу таким образом, чтобы, когда случится что-нибудь ужасное (по ошибке сотрутся важные файлы или рухнет система), юзер всегда мог "сделать шаг назад" и вернуть свой компьютер в то состояние, в котором он пребывал до выполнения роковой операции.

Домашняя бухгалтерия v 3.6

Windows 9x/Me/NT/2k
Size: 3023 Kb
Shareware
http://homesoft.agava.ru

Тебе никогда не приходилось, ощупывая пустые карманы, в которых еще вчера весело звенели монетки и шуршали бумажки, задаваться вопросом: "А куда, собственно, делась вся наличность, если я ничего такого не покупал?!!". Если приходилось, то, возможно, тебе стоит поближе познакомиться с "Домашней бухгалтерией". Эта прога поможет тебе внести ясность в свои финансовые дела. Она имеет русский интерфейс и интуитивно понятна. С ее помощью можно вести учет своих расходов и доходов, планировать свой бюджет и контролировать движение денег, которые были даны или взяты в долг. В "Домашней бухгалтерии" есть возможность вести все записи как в одной, так и в двух валютах. На основании этих записей программа способна строить отчеты и диаграммы, наглядно показывающие, сколько денег за определенный период у тебя тратится, скажем, на компьютер, сколько - на пиво, а сколько - на девочек. Также данные из "Домашней бухгалтерии" можно выводить на печать и экспортировать их в другие форматы (Word, Excel, Access, HTML, XML, Paradox, DBase). Я не знаю, поможет ли тебе эта прога разбогатеть, но за то, что она позволит тебе избежать ранней смерти и эпитафии на могиле: "Задолжал сколько сумел, всем кому мог", автор программы ручается :).



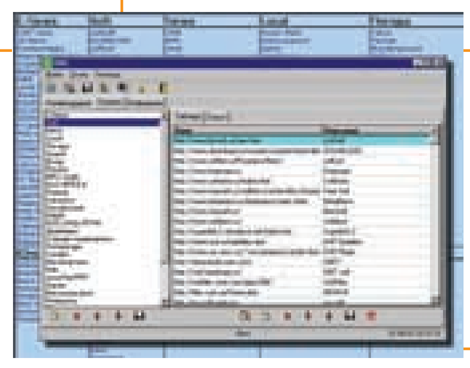
VoiceNet VRS 2000 v 1.3

Windows 9x/Me/NT/2k
Size: 5694 Kb
Shareware
http://www.groverind.com

Я всегда мечтал управлять голосом своим любимым компом. Приятно, знаешь ли, развалиться в кресле перед монитором, скомандовать: "Подключись к Сети. Проверь почту", а затем одним глазом лениво наблюдать, как машина суетится... VoiceNet VRS 2000 - единственная программа, которая смогла в полной мере воплотить в жизнь эту мою мечту. Другие (даже такие монстры, как IBM-овский пакет Via Voice и Naturally Speaking от Dragon Systems) не справились. Вместо того чтобы просто запомнить, как я произношу ту или иную команду, они выпендривались: пытались разложить сказанное мной на буквы, понять смысл... К сожалению, сделать это им никогда не удавалось (что, впрочем, не удивительно, ведь все команды они заставляли меня говорить по-английски! :). А VoiceNet VRS 2000 изначально наплевать, что и на каком языке ты говоришь, т.е., когда во время предварительной тренировки программа по-английски просит тебя произнести "File Save!" или, скажем, "Mouse Double-Click!!!", - смело диктуй в микрофон: "Сохрани" или "Кликни дважды". Прога запомнит твои варианты, после чего ты сможешь запускать приложения, расправляться с файлами, командовать окошками, "нажимать" кнопки на клавиатуре и даже... управлять курсором мышки исключительно голосом. Причем, при желании - не стесняясь в выражениях! :)

Start Page URL v 0.7.2

Windows 9x/Me/NT/2k
Size: 453 Kb
Freeware
http://yugres.al.ru



Клик по ссылке в IE или Опере с одновременным удерживанием Shift вызывает автоматическое открытие данной ссылки в новом окне. А теперь представь, что каждый раз, когда ты запускаешь свой веб-браузер, тот по умолчанию открывает HTML-страницу с линками на свои любимые сайты. Разве это не удобно? Ты же можешь быстренько "накликать" по интересующим тебя ссылкам, а потом, не спеша, переползать из окна в окно, изучая сайт за сайтом! Одна беда - для создания такой стартовой страницы требуется приложить определенные усилия, к чему большинство юзеров просто не готово. К счастью, я обнаружил, что эту проблему превосходно решает программа Start Page URL. Она позволяет максимально автоматизировать процесс создания и поддержания в актуальном состоянии страницы с коллекцией ссылок. Внешний вид такой страницы может легко настраиваться при помощи CSS, причем семь различных стилей оформления идут в комплекте с программой. Еще в том же комплекте находится очень солидный "базовый" набор ссылок, из которого легко формируется черновой вариант своей собственной паги. Ссылки и разделы, отсутствующие в наборе, можно добавить в базу данных Start Page URL вручную, скопировать через Буфер обмена, импортировать из ослика IE или текстового файла. Ну а насколько привлекательно выглядит сгенерированная этой прогой страничка, тебе, я надеюсь, удастся разглядеть на скриншоте.

iOpus STARR PC & Internet Monitor v 3.08 PRO

Windows 9x/Me/NT/2k
Size: 700 Kb
Shareware
http://www.iopus.com/starr.htm

Еще кто-то из классиков заметил, что больше всего люди интересуются тем, что их совершенно не касается. А поскольку наш журнал не ставит перед собой высоких целей перевоспитания человечества, то я решил включить в список "Необходимых вещей" программу, с помощью которой каждый юзер может удовлетворить свое любопытство и сунуть нос в дела ближнего своего. Называется эта программа STARR и является одним из лучших клавиатурных шпионов, который я когда либо видел. Никак не афишируя свое присутствие на машине, STARR берет пользователя под свой неусыпный контроль. Программа старательно отслеживает все нажатия клавиш (даже специальных!), регистрирует заголовки всех запускаемых приложений (и пути к этим приложениям!), делает регулярные "снимки" экрана и скрупулезно записывает адреса посещаемых юзером веб-сайтов. В зависимости от задачи можно использовать все функции STARR-а или только некоторые из них. Разумеется, как и положено любому приличному шпиону, STARR умеет отсылать отчеты хозяину на e-mail. В заархивированном виде. Причем не только по таймеру, но и по мере достижения отчетом определенной величины... Подробные сведения о способах незаметной инсталляции клавиатурного шпиона на машине "подозреваемого" находятся в руководстве... Кстати, если ты, приятель, дочитал до этого места, значит чужая личная жизнь интересует тебя не на шутку. Поэтому, вероятно, кроме STARR-а, тебе стоит взять на вооружение еще и программу Stealth Email Redirector. Незаметно установи ее на компьютере "подозреваемого", и в твой почтовый ящик будут исправно приходить копии всех отправленных этим человом писем. Возможность устроить свой собственный маленький СОРМ тебя привлекает? Тогда запомни адрес: www.softsecurity.com :).



МЫ ЖДЕМ ТЕБЯ!!!

– Если ты владеешь литературным слогом
– Если ты постоянно юзаешь *nix
– Если ты постоянно качаешь софт под *nix
– Если ты любишь ШароWAREZ
– Если ты хочешь работать с нами

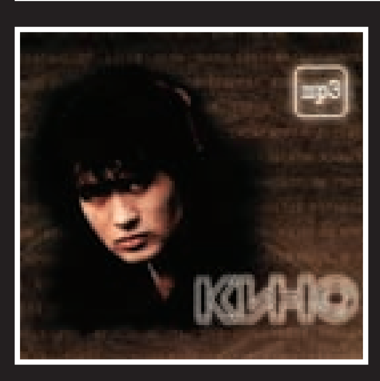
Тогда у тебя есть реальный шанс стать ведущим раздела UnixWAREZ.
Пиши и присылай пример статьи на sintez@real.xakep.ru



Музыка для крякера

Команда: Океан Эльзы (http://ocean.com.ua)
Пластинка: Модель
Релиз: Real Records, 2001
Реальный хит: Я до тебе

Уверен, что такая команда как "Океан Эльзы" тебе давно и отлично известна. Если же нет - то новый альбом "Океана Эльзы" - отличный повод для первого знакомства. Не переживай, что большинство композиций написаны на украинском языке, не пытайся установить точно что именно играет команда - рок или поп, лучше просто расслабься и прислушайся. Музыка тебя не разочарует.



Музыка для хакера

Команда: Кино
Пластинка: Сборник всех альбомов
Релиз: Moroz Records, 2000 (CD предоставлен магазином "ПУРПУРНЫЙ ЛЕГИОН" www.plegion.ru)
Реальный хит: Каждый второй...

Обрати на этот "двойник" своё пристальное внимание. Фирменные компакты, на которых собраны все альбомы действительно легендарной группы в формате mp3, а также обложки альбомов, фотографии. Качество музыки более чем достаточно для прослушивания на компьютере, композиции закодированы с битрейтом 192 и позволяют насладиться песнями "Кино" в самой полной мере.



Музыка для западлостроителя

Команда: Ногу свело! (www.nogu-svelo.ru)
Пластинка: Бокс
Релиз: Grand Records, 2000 (CD предоставлен магазином "ПУРПУРНЫЙ ЛЕГИОН" www.plegion.ru)
Реальный хит: Последнее танго

"Оправдываться поздно - я замечен, лечиться тоже поздно - я убит" - примерно так я ощущал себя в момент первого прослушивания альбома с весёленьким названием "Бокс". Сам по себе альбом звучит задорно (хотя и не порно :)), песни яркие, запоминающиеся и позволяющие забыть хотя бы ненадолго о засильи всесильной попсы, посредством которой гадят нам в уши разные там продюсеры и шоу-мены. Долой попсу! Даёшь "Ногу Свело!"

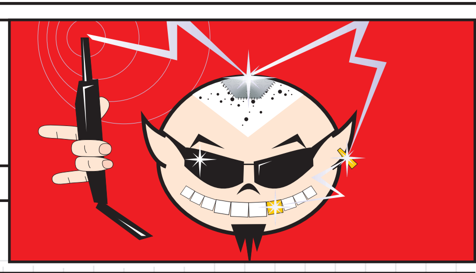


Музыка для warezника

Команда: Jah Division (http://jahdivision.rinet.ru)
Пластинка: Не пластинка, а первый CD!
Релиз: Информация разглашению не подлежит :))
Реальный хит: Cubana Dub

ДЖА РАСТАФАРАЙ! Ты что-нибудь слышал о растаманах? Ну, про Боба Марли, Ямайку, дреды, позитивные вибрации, солнечный раста-рэггей? В таком случае тебе должен понравиться первый, самый настоящий компакт-диск, заполненный до отказа "русским рэггеем" от отечественных монстров жанра - команды Джа Дивижн. Послушав сам диск, можно сходить и на концерты группы, расписание которых и все подробности ждут тебя на сайте группы.

FAQ



Stepan Ilyin vs BX (faq@real.xakep.ru)

С какими базами данных можно работать, используя php?

Если ты еще только собираешься осваивать навыки web-программиста и не знаешь, с чего лучше начать - с php или perl, но уже сейчас предполагаешь, что будешь активно работать с базами данных, то можно смело выбрать php. Одним из главных плюсов php является возможность работы с огромным количеством баз данных: Adabas D, InterBase, PostgreSQL, dBase, FrontBase, Solid Empress, mSQL, Sybase, FilePro (только чтение), Direct MS-SQL, Velocis, IBM DB2, MySQL, Unix dbm, Informix, ODBC Ingres, Oracle. Думаю, есть из чего выбирать, но я бы остановился на sql.

Какие команды мне необходимо знать для работы с базами mysql, используя php?

В общем, не зря mysql+php называют неразлучной связкой - работать с mysql через php не только очень эффективно, но и элементарно. Так что, выучив ниже написанные команды, ты больше не будешь пугаться слова SQL.
1) подключение к серверу MySQL
mysql_connect ("$hostname:$port", "$username", "$password");
2) выбор базы данных (database)
mysql_select_db ($dbname, $openConn2db);
3) создание запроса (query) к базе данных
$queryResultID = mysql_query ($DBquery, $openConn2db);
4) определение количества полей (number of fields) в результате запроса
mysql_num_fields ($queryResultID);
5) определение количества строк, возвращаемых запросом
mysql_num_rows ($queryResultID);
6) создание массива со строками результата
mysql_fetch_row ($queryResultID);
7) выборка данных из первого элемента массива
current ($correspondingRowArray);
8) выборка данных из следующего элемента массива
next ($correspondingRowArray);
6) закрытие соединения с сервером MySQL (mysql_close)
mysql_close ($connLinkID);



Вышла финальная бета Office XP. Что можешь посоветовать - ставить или нет?

Финальная бета действительно вышла и оставила у меня приятные впечатления. Установка прошла очень быстро, а количество задаваемых установщиком вопросов было минимальным. Первое и, пожалуй, главное замеченное отличие - это внешний вид свежего софта. ИМХО, работать стало приятнее, и это новшество не может не порадовать. Так что если собираешься уговаривать босса купить пару лицензионных Office XP (как водится, ставим скачанный варез, а бабло на лицензы ныкаем себе :), то покажи ему новый интерфейс - наверняка, купит :). Реально новая фишка - "smart tags" (в переводе с английского означает "умные теги"), которая в скором наверняка станет неотъемлемой частью форматирования текста. Правда, воспетые встроенные системы альтернативного ввода текста при помощи микрофона или пера меня не привели в восторг. Пера в наличии не оказалось, а вот фичу с микрофоном я попробовал, и результат был, мягко сказать, не очень: или мне мою английскую дикцию фиксить, или Microsoft'у еще предстоит БОЛЬШАЯ работа над этой фишкой. В общем, поработав на Office XP, было принято решение о полном переводе офисных дел из 2K`ея в свежий eXPerience.

Недавно поставил linux. Мне он не понравился/он жутко неудобный/у меня программы не компилятся/и вообще такая фигня. Как его можно удалить?

ОЧЕНЬ частый вопрос - прежде чем ставить пингвина, ты наверняка читал, что простого в *nix'ах ничего не бывает, linux изучить - не винду поставить, так что надо было быть готовым к трудностям, с которыми можно встретиться. А когда эти трудности появляются (а они 100% появляются), надо не linux удалять, а идти за rtfm, на irc, форумы, конференции, к профи и искать ответ на вопрос. В общем, если ты подписал смертный приговор Туксу, то бери fdisk из директории виндов и запускай его с ключом /mbr, тот заменит 1 сектор твоего харда, тем самым остановит жизнь lilo (linux'овский загрузчик). Теперь стартанет уже ставшая родной винда. Только вот свободного места ни на байт не прибавится. Дальше возникают два варианта: воспользовавшись Partitision Magic, перевести линуксовый раздел в фат или с помощью fdisk'a удалить non-dos (не досовый) раздел, а затем создать стандартный.

Что значит банить по маске? Зачем нужна эта фишка, ведь можно без проблем создать бан через менюшку irc-клиента?

Представим ситуацию - на твоем канале хулиганит перец, который сидит на диалапе, ты банишь его с помощью своего c00l-хацкерского скрипта, который по умолчанию настроен на "бан по серверу". Результат - никто из юзеров этого же провайдера зайти не сможет! Поэтому бан тоже надо уметь выбирать - или по серверу, или по хосту, или же по иденту.
Здесь и потребуется прописать бан по маске. Общая маска выглядит так: nick!ident@host.server. Например, в моем whois'е ты увидишь примерно следующее: step!step@174.pool.kaluga.ru. Забанить меня можно следующими способами =):
по нику - *step*!*@*
по иденту - *!*step*@*
по хосту - *!*@174.pool.kaluga.ru
по серверу - *!*@*.*.kaluga.ru
Очень часто используются смежные вариации, например:
по иденту и хосту - *!step@174.pool.kaluga.ru
по нику и серверу - step!*@*.*.kaluga.ru

Как установить win98/Me поверх win2k?

Многие, начавшие работу с win2k, часто задают этот вопрос, который кажется им неразрешимой задачей. Однако поставить win9x/Me поверх win2k совсем несложно. Есть правда один нюанс - раздел "c:", а также раздел, зарезервированный под Win98/Me, обязательно должны быть в fat'e. Если так и есть, то в дальнейшем проблемы у тебя навряд ли возникнут. Создай загрузочную дискету win2k (надеюсь, ты знаешь, как ЭТО замутить), а также дискеты с ERD, запустив утилиту makeboot.exe, которая по умолчанию есть в любом дистрибутиве win2k в папке bootdisk (кстати, ERD - это дискеты экстренного восстановления). Тебе также понадобится загрузочный CD дистрибутива win98/Me. Выполнив описанное выше, можешь стартовать с загрузочного CD и начинать установку win98/Me. Последнее действие не должно вызвать проблем. Поставил? Теперь необходимо прогрузиться с boot-дискеты Windows2K. Когда система предложит тебе вариант загрузки, укажи ей опцию "Восстановления поврежденной установки Windows 2000" (на буржуйском: "Repair damaged Windows 2000"). Система захочет поиметь каждую из ERD дискет, так что тебе придется вставлять их во флоп по очереди. В итоге загрузочный сектор будет восстановлен, и при перезапуске компа появится всем знакомая менюшка выбора операционки. Если вдруг что-то восстановилось криво и столь ожидаемая менюшка не появилась, тебе придется вручную добавить строку "C:\="Microsoft Windows" в файл c:\boot.ini.







У меня двухпроцессорная мамка, правда, на ней стоит только один процессор (а жаль ;), но BeOS почему-то не загружается. Пробовал на другой матери - все оК.

Действительно, у многих счастливых обладателей двухпроцессорной мамки, однако владеющих лишь одним процессором, часто появляется проблема с загрузкой BeOS'а. Но пофиксить баг очень просто. В bios'е (не в BeOS'е =) найди опцию "MPS for single processor". Смело отключай ее. Проблема исчезнет, зато появится другая, не менее глобальная: теперь NT не захочет грузиться, пока ты не вернешь выше написанный параметр в исходное положение. Решил бросить понты, купив двухпроцессорную мамку? Теперь помучайся... =)

Мне подарили UPS, но инструкция на английском. Не подскажешь - что обозначают термины sags, brownouts, spike, surge?

Во подарки делать начали... может и мне подарят? А слова, которые ты привел, даже к компьютерной терминологии не относятся, так что в следующий раз ищи ответ в специализированных словарях.
Sags (Brownouts) - кратковременные понижения напряжения в питающей электросети. Наиболее частая проблема.
Blackout - полное исчезновение напряжения в питающей электросети.
Spike - кратковременный высоковольтный импульсный выброс напряжения в электросети (длительность - миллисекунды).
Surge - кратковременное повышение напряжения в сети, продолжительность 1/120 сек. и более.

Как я могу потестить свой хард на скорость, надежность и т.д.?

Софта для тестирования довольно много, но достойные экземпляры найти крайне сложно. Я не буду упоминать специализированные тесты от производителей винтов, а предложу лишь одну фичу и добавлю пару линков на другие, что помогут тебе получить общее представление о различных параметрах твоего харда.
HDDSpeed *(http://xponik.spb.ru/hddspeed/)* - я не случайно начал именно с этой проги, т.к. сия утилитка завоевала доверие многих гуру, и пока, на мой взгляд, альтернативы ей нет. Распространяется бесплатно с открытыми исподниками, что сразу радует (уже загорелся желанием написать свой коммерческий тестер? =). Поводом юзанья проги может стать то, что она написана русским кодером (хе-хе, типа, Russia - ru11Ezz 4ever). Столь серьезного набора функций, имхо, нет ни в одной подобной проге. Данный тест позволяет получить как информацию о физических характеристиках конкретной модели жесткого диска, так и о скорости его работы в системе. Кроме того, можно визуально оценить состояние поверхности диска и определить наличие плохих блоков (bad blocks), замещенных дорожек (remapped tracks) и плохо читаемых участков. А с версии 2.0 появилась фича "лечения", так что ты сможешь юзать эту утилиту для реанимации своего харда, правда, я сильно сомневаюсь, что она справится с поставленной задачей лучше, чем специализированные проги от производителя твоего винта. Нельзя не упомянуть о возможности построения графика линейной скорости чтения на разных дорожках диска. По графикам можно отследить локальные дефекты поверхности, а также определить, достаточна ли пропускная способность контроллера/шины для данного жесткого диска. В общем, программа - супер, правда, минус у нее все же есть - она работает только под DOS`ом, причем автор рекомендует создать тесту определенные условия (читай прилагаемый rtfm) для еще большей точности при диагностике.
Другие - **Drive** *(http://xponik.spb.ru/drive/)* и **ThreadMark** *(http://www.acnc.com/benchmarks/)*.





Даниил Шеповалов
(dan@real.xakep.ru,
www.danya.ru)

Как избавиться от бои-френда

Респект тебе, надежный как трах... дотянись до лазера. Хотя мы, вообще, сегодня не об этом. И не о скромном быте смазливых педерастичных морячков-папаев, как уже скорее всего решили самые эрудированные читатели, бросив ясный взгляд на название атикла.

Сегодня, пацаны, я сделал всем нам реальную подставу. Сегодня, первый раз за свою жизнь, я написал статью, которая посвящена исключительно девушкам. (Акела промахнулся! Акела промахнулся! - прим. мертвого слоника по кличке Смайл). Но я все могу объяснить (что-то последняя моя фраза чересчур попахивает дешевыми сериалами). Вот смотри, почему я вообще не хочу иметь детей? Если родится мальчик - это клево, можно будет воспитать его настоящим мужчиной, ходить вместе на рыбалку, пить березовый сок на набережной, в общем, все дела. А если девочка? Тогда через 17-19 лет она превратится в ослепительную половозрелую красавицу и.... КАКОЙ-ТО КРЕТИН БУДЕТ ЕЕ ТРАХАТЬ!!! Ты только представь: мою милую дочурку, принцессу, рыбку будет пошло иметь во все места какой-то озабоченный волосатый урод (Сам урод! - прим. ослика Феди). Девушки, опомнитесь! Перестаньте отдавать свою любовь и тело всем этим потным мужланам, эмоциональным кастратам и фригидным компьютерщикам. Подумайте об обливающихся кровью сердцах ваших отцов. Воспользуйтесь приведенным ниже священным мануалом по киданию бой-френда и поживите в гордом одиночестве лет 8-10. А потом вы все равно уже никому не нужны будете...

1. Кончай его

Лежа с ним в постели после страстного и бурного секса, когда он уже находится в полусонном

благостном состоянии а-ля "Welcome to Nirvana", начни жестко и настойчиво грузить его на тему вашего материального благосостояния и светлого будущего. Скажи: "Дорогой, у нас ведь будет много детей, правда? Наверное восемь... а может даже и все десять. Я буду целыми днями их нянчить и хлопотать по хозяйству. А ты будешь зарабатывать деньги и приходить вечером в наш уютный домик на Лазурном берегу, ко мне и детям. Только, милый, тебе придется очень много работать. Я не хочу всю жизнь прожить в этом обшарпанном сарае вместе с твоим гуимпленом-братом. Так что ты должен стать как минимум членом совета директоров крупной корпорации. Я уже выкинула все твое пиво из холодильника, спустила в туалет сигареты и сказала твоим друзьям-тунеядцам, что ты больше не желаешь их видеть. Я правильно поступила, котик? Да, и перестань шляться по этим сомнительным клубам и вечеринкам. Ты ведь прямо завтра уже должен начать готовиться к своей новой блестящей карьере. Кстати, твои билеты на футбольный матч "Спартак - Зенит" я поменяла на театральный абонемент для нас двоих... Я подумала, что театр серьезно расширит твой кругозор. Ну скажи, что я у тебя умница! Что ты все молчишь да молчишь, поговори со мной!".

2. Павлик.ру

Я думаю, сладкая моя, что в твоей жизни был далеко не один замечательный мальчик. Так вот, ты слегка напрягись и вспомни само-

Ты только представь: мою милую дочурку, принцессу, рыбку будет пошло иметь во все места какой-то озабоченный волосатый урод (Сам урод! - прим. ослика Феди). Девушки, опомнитесь!

го-самого замечательного из них. Допустим, его зовут Павлик (Не-а, его зовут Ашок Тураганян - прим. ослика Феди). Теперь твоя задача: постоянно упоминать имя этого Павлика всуе, сравнивая его несравненные достоинства с жалкими



характеристиками неугодного бой-френда. Чтобы тебе легче было понять, как именно себя надо вести, я приведу ниже ряд примерных фраз, которые тебе следует периодически как бы невзначай бросать своему надоевшему дружку:

"Павлик бы за пять минут починил эту злосчастную машину. А у тебя руки просто не из того места растут."

В постели: "Ты слишком груб и нетерпелив. Вот Павлик... он



часами доводил меня своими ласками до исступления. Как только вспомню эти горячие волны, которые по десять раз за ночь поднимали меня на вершину блаженства... ооо... С тобой же мне постоянно приходится имитировать оргазм, жалкий лузер".

"Павлик умел себя вести в порядочном обществе, не то что ты - тупая деревенская свинья".

"Нищий скупердяй! Павлик всегда оплачивал мои телефонные счета".

"У тебя абсолютно нет вкуса - я стесняюсь идти рядом с тобой по улице. Вот Павлик - он знал толк в модной одежде".

Ну а после нескольких дней подобной терапии тебе следует добить неугодного мальчика. Во время вашей сладкой прелюдии на раскладном ложе любви достань припасенный заранее

Девушки, я безумно виноват перед вами. Я моральный урод и пишу для точно таких же моральных уродов, которые считают вас ограниченными похотливыми дурочками. А все дело в том, что мы, мужчины, попросту избранные инопланетяне-десантники, которых заслали на вашу, женскую, планету с загадочной миссией... вступить с вами в КОНТАКТ...

штангенциркуль и, измерив по всем параметрам достоинство бой-френда, печально произнеси: "Здесь Павлик тебя тоже серьезно обскакал".

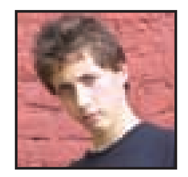
3. 9 с половиной недель

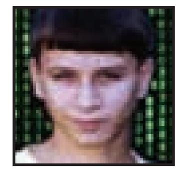
Приготовь побольше взбитых сливок и пообещай своему мальчику чудесную ночь любви. Без обмана. Поставь романтическую музыку, зажги свечи и нежно покрой интимные и не очень места своего Ромео этим шедевром кулинарии. Ну а затем, естественно, начни мега-сексуально слизывать с него сливки. Так и быть, пусть он покайфует минут пять, а когда ты практически доведешь его до пика наслаждения, тут же сунь два пальца в рот и блевани ему на грудь со словами "Я давно тебе хотела показать, что меня от тебя физически тошнит". Думаю, временная импотенция и серьезный психический срыв ему обеспечены.

4. Девушки бывают разные...

Начни серьезно интересоваться компьютерами. Покупай умные книги вроде "Архитектура RISC", "Программирование для встроенных систем", "PERL с нуля" и усиленно делай вид, что ты их с интересом читаешь. Перестань использовать косметику, вообще следить за собой (я понимаю, что сложно, но надо себя пересилить - это все временно). Также будет крайне замечательно, если ты начнешь принимать водные процедуры раз в одну/две недели и начисто забудешь слово "эпиляция". Полностью возьми в свое личное пользование компьютер бой-френда. Получи поинта или ноду в ФИДО и тут же с головой окунись в FTN-жизнь. Ходи абсолютно на все поинтовки и сисопки, проводи горячие ночи за чтением почты (а не с ним в постели) и полностью перейди на компьютерно-фидошный сленг. Питаться следует исключительно чипсами (вообще забудь про слово "кухня") и пивом. Бутылочки три-четыре девятой Балтики у компьютера - это как раз то, что тебе нужно. Свое общение с бой-френдом сведи к минимуму: при любой его попытке завести слю-

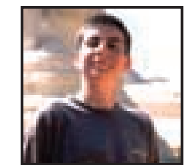
МЫ ЧИТАЕМ ХАКЕР


~PrAsS~


NAJORT

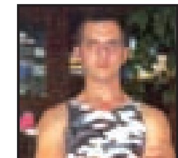

[Stim]

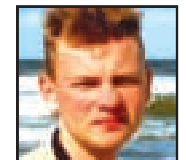

brAUnd


BLAST

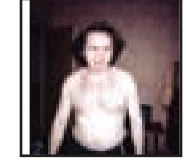

Hem


Коля и Амир

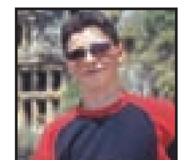

КРУТ


FefazeR

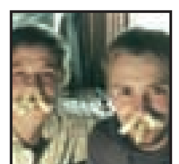

AcTpoyM

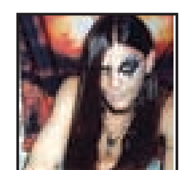

Grey Cat


(:grundic:)

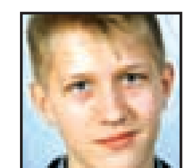

ZERK

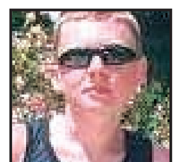

sash


Spherix & Roland


Maxoт


Metal Invader


GUS

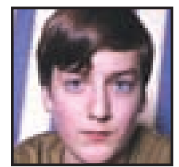

Mr.Nick

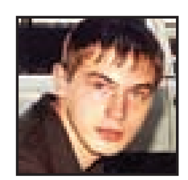

nikolich

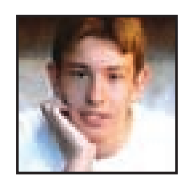

bagiMOT

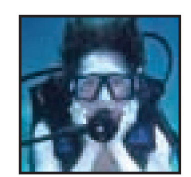

Oleg

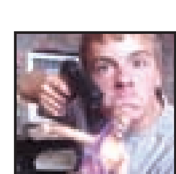

Ozon

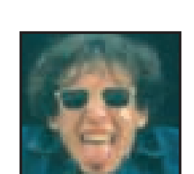

SHuRuP

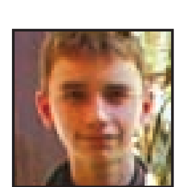

SONNIE


Poppin@Good


Leshk@

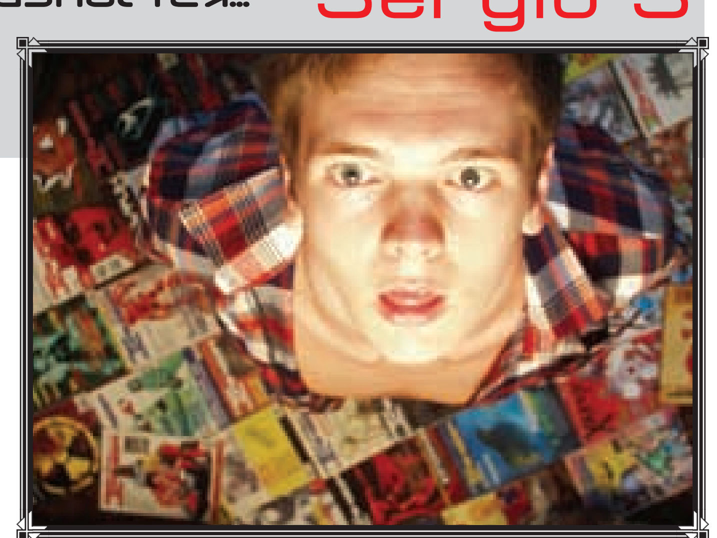

warfish


Stemir


$AUzzz Pnoac

И Мистером SUPERSTAR признается... Sergio S

Вглядись в эту фотку! Чел не только все клево снял, но к тому же является одним из наших старейших читателей. Все номера, леди и джентельмены! Все!





ты еще можешь попасть на страницы Х!

Пришли свою фотку и ник на адрес magazine@real.xakep.ru, с сабжем "SUPERSTAR". Чем больше размер фотки и чем она качественне, тем лучше.
Предупреждение: мы напечатаем только твою фотку и ник. Для объяв юзай борду на последней странице!

сигнала. Следует начисто отказаться от реального секса: пусть твой мальчик застанет тебя пару-тройку раз мастурбирующей на откровенные фотографии породистых самцов с pornoz.com. Ну и неплохо будет пофлиртовать в icq/irc с десятком-другим "Вольдемаров". Что? Твой бой-френд не повесился и все еще живет с тобой под одной крышей? Тогда прости его - он исправится.

5. Все уже изувечено до нас

Проведи ночь вне дома и, явившись под утро к бой-френду, кинься ему на плечо и зарыдай. Вперемешку с соплями, слезами и губной помадой говори что-нибудь вроде: "Ну вы, мужики, и уроды... Кобели... Вам лишь бы добиться своего, а потом хоть трава не расти... Вот зачем утром вы телефон спрашиваете и делаете вид, что записываете... Ведь не позвоните больше никогда... Вот и сегодня... Тоже спросил... И ты, наверное, тоже бедным девочкам не звонишь... Урод... Не трогай меня... Не трогай, я сказала!!! Сам успокойся, животное."

6. "Как там было у Кафки...", – задумчиво протянула Наташа

Несколько месяцев не вылезай из библиотеки им. В.И. Ленина. Прочитай всю графоманскую писанину Ницше, Канта, Шопенгауэра, Юнга, Фрейда, Кафки, Джойса, Сартра, Кизи, Лири и прочих инвалидов интеллектуального труда (полный список возьми у своей знакомой Наташи... да-да, у той заумной уродины в очках из литинститута). Если в ответ на предложение бой-френда "давай сзади" ты сможешь разразиться десятиминутной тирадой о правах женщины, скрытых сексуальных комплексах приятеля, натурфилософии, наладке позитронных ускорителей и роли Будды в развитии духовной мысли Японии, то мой тебе респект - вылезай из библиотеки. Твой бой-френд сам убежит от тебя через два дня, навеки приобретя интергалактический комплекс неполноценности. Ну а чтобы восстановить душевное равновесие и преждевременно не уйти из жизни - пару недель занимайся непрерывной сексуальной терапией: книжное дерьмо из головы можно только вытрахать. Главное - ни в коем случае не разговаривай со своими партнерами, шифруйся под дурочку, чтобы они не смылись от тебя досрочно.



Секс без причины – признак мужчины

Девушки, я безумно виноват перед вами. Это я написал "Как избавиться от подружки", "Самый правдивый женский гороскоп" и прочие труды, пропагандирующие тотальную дискриминацию по половому признаку. И ведь сколько еще всего напишу! Заранее простите меня, пожалуйста: эта статья канает за отмазу? Я моральный урод и пишу для точно таких же моральных уродов, которые считают вас ограниченными похотливыми дурочками. А все дело в том, что мы, мужчины, попросту избранные инопланетяне-десантники, которых заслали на вашу, женскую, планету с загадочной миссией... вступить с вами в КОНТАКТ...

Нам пишут психи

(самое шизанутое письмо для Дани)

О, приветствуем тебя, Трижды Будда Советского Союза. Пишут тебе неудовлетворенные студенты из Одессы. Преклоняемся перед твоим талантом неординарного мышления по отношению к сексу. Мы много раз пытались испытать Оргазм Робокопа, но так ничего и не получилось. Мы даже пытались засунуть себе кабель модема в задницу и совокупиться с киберпространством, но кроме CONNECT 2400 ничего не вышло. Потом мы долго старались онанировать сквозь отверстие открытого CD-ROM'а, но это было довольно проблематично, потому как CD-ROM имеет тенденцию периодически закрываться. Один наш друг пытался получить оргазм от струи знойного теплого воздуха, веющего сквозь дырку в блоке питания. Никогда не забудем выражение его лица, когда его "balls" стало наматывать на кулер. Потом мы осознали, что Оргазм Робокопа лежит вне понятия "обыкновенного" секса, и решили ударится в струю пирсинга: вшивать перемычки под кожу, засовывать бипер в прямую кишку (за отсутствием бипера пользовались саббуфером) прикладыванием к интимным местам процессора INTEL80286, разогнанного до частоты 2,2 ГГц. Но все, как всегда, окончилось неудачей. Мы решили пойти еще дальше вплоть до трансцендентного садомазохизма. С криками: "Теперь я буду повелителем!!!" - все вышеперечисленные методы мы стали проводить над своими девушками. От чего те с криками, визгами, воплями, слюнями, соплями, серой из ушей и тому подобными жидкостями из разных отверстий тела стали от нас убегать и прятаться. Совсем расстроившись, кончив на материнскую плату (от чего она и сгорела) и забив ржавый строительный гвоздь себе в копчик, мы решили попросить помощи у Самого. Пожалуйста, объясни непосвященным, как нужно жить полноценной сексуальной жизнью.



Наше мыло: magazine@xakep.ru

Солнце ласково зашло над рекой Хуанхэ, вздыбили горбатые спины усталые хунвейбины, добрейший сын Куаки DramN! Кстати, как поживает несравненная Куяка, не собирается ли на заслуженный отдых? Волнуемся мы тут за нее, куячит ведь и куячит, старая, без сна и отдыха... Хорошо ли спит старик Полмпилус? Как у него стул? Наши все ему кланяются, особенно непобедимый Добрянский. Он тут недавно хотел сделать харакири, но немного не рассчитал... пришлось ему принять иудаизм.

Ну, а что касается твоего вопроса - "ето чистая проавда", как ни печально сознаваться в этом, наслаждаясь первыми лучами желтолицего светила... Йокка Хомякадзе, самурай-прогульщик.

From: yzbek [yzbek@ok.kz]
Subject: [empty]

Здравствуйте, многоуважаемая редакция!, Вы молодцы, инфы в самый раз. Окей, откинем болтологию в сторону, ваш журнал и ОСОБЕННО спецвыпуски помогли в моей жизни. Теперь я уже другой человек, раньше кроме компа и никого не признавал, и не знал. Благодаря вашему журналу я избавился от врагов!!!!, нашел себе любимую девушку, получил работу. Теперь жизнь изменилась. Все отлично, спасибо в помощи!!!!! yzbek

Ответ X:

Мир твоей сакле, многоуважаемый!
Что ж, твои слова пролились на наши души живительным бальзамом. Я уже давно всем пытался втемяшить, что с помощью X можно не только перезнакомиться со всеми и уничтожить посредством удаленного западлостроения всех врагов поголовно, но и остаться на ПМЖ у любимой девушки, просто поставив на ее домашний компьютер Windows 98. А вообще-то, настоящему коту и в декабре март, так что держи хвост пистолетом, задний проход закрытым, а X открытым и доступным всегда и везде и в любое время. Твой юный Горбздик (Горбачев, защитник демократии и культуры)

From: Чума Крутой [Chuma-Super@rambler.ru]
Subject: Vzlom xakep.ru

Hello, хакеры!
Типа у нас с GIFом (ГИФом а не джифом) большой к вам плизз. Целыми ночами не спали, ваш сервак ломали. Прямо выдохлись!!! Троянов засылали, сканером сканили, скрипты разные пробовали, атакой отказ от обслуживания пользовались, а ваш сервант никак не ломается! Мы уже все пробовали, подскажи что-нибудь!

ЗЫ: Нам, между прочим, Microsoft ломать было проще!

Ответ X:

Так вот, ядрена BOSH, кто к нам ломился! А мы уж думали, что это объявился тот самый мальчик, которого в джунглях воспитали дятлы, и он всех потом задолбал. Короче, прощайся с друзьями и срочно закупайся полноприводной инвалидной коляской и фильтрами для базара. Центнер уже вышел на твой след... Иван Сусанин. Редактор "Словаря польских нецензурных выражений".

From: Kryo@xakep.ru
Subj: Очень просим!

Здравствуйте, много многоуважаемая редакция X! Пишут вам малоуважаемые ученики средней школы #31337 города Пупкина. Дело в том, что наши учителя информатики, когда мы показали им X (в смысле журнал Хакер, а не то, что вы подумали), они сказали, что все это - происки искусственного интеллекта. Мы, естественно, на них обиделись, и после этого школьные компьютеры стали работать очень X (уже не в смысле Хакер, а то, что вы подумали). Тем не менее, очень просим выслать к нам в школу делегацию в составе Холода и Данечки Шеповалова для внесения веры в темные головы наших информатиков. Даня будет вгонять, он это умеет, а Холод пусть будет у Дани личным шофером (может он остальных наших учителей и училок подавит). На этом оквадративаемся, всем до свидания!

Ответ X:

Здравствуйте, наши дорогие пупкинцы!
Мы тут посовещались с товарищами и решили выслать вам на подмогу спецподразделение энциклопедиков, усиленных кем надо. Вы только не волнуйтесь и никогда больше не показывайте X вашим учителям информации, иначе вся подготовленная бессонными ночами операция провалится и наш план будет раскрыт. Помните, что наших секретных агентов можно будет узнать по зажигалкам Zippo и огнетушителям UnZippo с лого X на борту. Ну, внучки, а сейчас ложитесь почивать, одеяла и подружки ждут ребят. Не поминайте лихом. Старик Катионыч да бабка Шухеризада.

From: egor [djay@xakep.ru]
Subj: Лично! В кулхацкерские руки!

Здравствуйте, мои маленькие дорогие любители спорта... и пива. Пива пива - уже наслушался, насмотрелся, напился в конце концов. Смотришь ящик и офигеваешь: *Ты где был - пиво пил*, *Хочешь я угадаю, хочешь, хочешь* и т.д. Не... я люблю пиво (хотя и сказал, что напился). Но нахрена столько рекламы этого хмельного напитка!!! Я к чему клоню...(ослика Дани :)) Мне хочется увидеть вместо этого рекламу моего любимого журнала, нет не PLAYBOYя, а что бы вы думали - ХАКЕР. Тогда бы этот журнал увидел по-настоящему жись! Ой, сколько бабла бы вы загребли.. ой... Ведь рекламируют всякий отстой типа "Бииип!" или "Бииип!". Скорее всего, и хакер подешевел бы (журнал). Я понимаю, что для рекламы нужно тоже немало бакинских комиссаров, но все же! Или знаете, еще лучше: сделайте какой-нить праздник хакера! Устройте концерт: позовите супер рульных диджеев, Била Гейтса, в конце концов изнасилуйте Даню внутрипопочно по очереди прямо на сцене! Успех будет грандиозный!!! Вывод. Всем будет хорошо: вам - лавэ, нам - отрыв и Дане - полное удовлетворение :<)! Так что все в ваших руках. Пора выходить за пределы Интернета и редакции! <Сводный брат ослика Дани>

Ответ X:

Даю подробные разъяснения по первому вопросу: реклама и нас порядочно достала, но мы ответим своей рекламой на вражью! Пусть буржуины знают, что "молоко вдвойне смешней, если трескать с огурцом", а подруге своей смело передавай, что "любой понос, любая менструация - все выдержат колготки "Грация". И будь внимателен! В компании с "Толстяком" пиво выходит незаметно! Ну, а если серьезно, то как раз в тот момент, когда ты будешь читать этот номер, на MTV уже во всю будет вращаться ролик X. Следи за рекламой!

На письма отвечал Centner

А что касается мысли устроить грамотную Х-Тусу, то однажды мы это обязательно забацаем. Забацаем так, чтобы всем на зависть и удивление. Это нам как два байта переслать! А ты пока что думай, каким образом и где предпочтительнее увеселяться, кто из ДЖ должен стоять за пультом и кого из менестрелей пригласить на сцену. Ты, в общем, думай, а я пойду получу много $$$$$, чтобы их на тусе все потратить. Ты тоже хочешь? Ладно, жми на клавишу Shift и, удерживая ее, - клавишу F4. The Падло Пикассо - художник-пофигист.

From: LCD [lcd_z@mail.ru]

Subj: Срочно в номер!!!!!!!!!!!!!!!!

Привет, компания хакеров; люди, надо срочно что-то делать, сегодня посмотрел программу совершенно секретно про оборону нашей страны и столько узнал, что аж страшно, оказывается американцы уже давно нас спонсируют, и что в замен, как вы думаете?, а они взяли и на сайте Пентагона выставили карты нашей страны с точными координатами военных заводов и даже шахт с ракетами; ребят, вы хоть бы там поломали их сайт (Пентагоновский), а то что делается такое, нас уже совсем ни во что не ставят, можно хоть сейчас идти и любой завод взрывать… И вообще, сломайте все буржуйские сайты, что бы не повадно было….. До свидания, LCD

Ответ Х:

Стрейфиться не надо, Лада! Нас не запугать просто так. Граница на замке! Но, тем не менее, ты смотри, гады, что творят! Ну ничего, мы уже сообщили куда не надо, нужные кнопки и рычаги нажаты, все шахты и ракеты мы срочно поменяли местами, а вместо заводов понаставили полевых сортиров и сменили номера на всех автобусах и трамваях. На всякий случай мы капитально засекретили Холода, теперь его позывной "Кирдык", а Добрянскому досрочно присвоили звание "полкового овощевода" второй статьи. Также в редакции Х прошли двухдневные учения под кодовым названием "Абзац" и "Пинцет", где отработаны все необходимые на случай внезапного удара навыки. В следующий вторник с боевой песней "По полу тапки грохотали" мы выйдем в дальний поход и… обещаю тебе, стяжаем всю возможную славу на полях виртуальной войны. Командир отдельного истребительного противосерверного лихеро-водочного батальона плаврук М.У. Дазвонов.

Самое ДУРАЦКОЕ письмо номера:



From: DramN [shabiev@bashnet.ru]
Subj: Надо выяснить!

У меня преподаватель есть Кормильцев, так вот его сын куаки японял играет в Наутилусе Полмпилусе! Проавда ли ето?

Ответ Х:

Птицы щебечут с утра, восхищаясь рассветом,
Солнце встречая…
И гадят, и гадят…
(из посвящения отважному самураю-куякинцу DramN-у)







Внимание ! Все, кто знает крутые функции Win32Api для VB пишите мне на xakep@gold-mail.ru Вышлю списки известные мне – 52 функции для всех целей (форматирование харда, выключение компа и т.д.).

Челы, кому нужны кряки и key-генераторы – мыльте на stan@krovatka.net – помогу!

Все кто юзает BeOS откликнитесь! :)
С уважением, Василий НаеБулкин (lex_31337@inbox.ru)

Привет народ! Как насчет интересно побщаться на тему аниме? Жду!
dark_home@rambler.ru

Ищу учителя по созданию 3D персонажей. Желательно из Минска. Если мне понравятся твои работы буду приходить на занятия. Заплачу!!! Шли работы на KillerMaxxx@mail.ru

Куплю видяху GeForce2 GTS (Gigabite) 64 меговую. До 150 баков. Все предложения на мыло. paralon_crew@rambler.ru

Все кто юзает Delphi 5.
Помогите. haldey@inbox.ru

Набираем мемберов в хак-группу NLSO. Ищем крякеров, хакеров, кодеров и вообще хороших людей... Все подробности на #NLSO, а также пишите мне на мейл. (demos@xakep.ru)

Кто знает, как устранить конфликт драйверов звуковухи Creative SB Live Platinum и тюнера PV 951 от Media Forte? Мыло: presto99@mail.ru

Учусь кодить на Дельфи5, ищу братьев по разуму и увлечению. Давайте переписываться! Моё мыло: kryo@xakep.ru

Помогите кто знает как настроить (ОС FreeBSD) X-Window под видео карту ASUS V7100 GeForce 2MX (x-cyas@mail.ru).

Приму в дар любую хак литературу. Шлите на мыло договоримся. marksuk@onego.ru

Киньте ссылку на электронного вида текст У.Гибсона – "Идору".
CyberpunkClub@pisem.net

Информационному агентству AK&M срочно нужен бот для повышения оперативности инфы на сайте экстремального спорта (относящемся к агентству AK&M).
функции бота:
1)генерация хтмл-а
2)размещение фотографий заданного размера на свежесгенерированной странице
3)размещение текстовых материалов на свежесгенерированной странице
Оплата гарантирована
предложения е-мыльте на a-girl-ru@xakep.ru

Кто хочет перепечатываться про хак, пишите... Hurmer@mail.ru

Привет чуваки! Я создаю музыкальную группу! Кто хочет вступить? Мыль на vovnem@online.com

}{акеры города Новосибирска объединяемся! Мыльте на duches@xakep.ru

Привет ищу друзей по переписке!!!
processorAL@mail.ru

Хочу обмениваться инфой по программированию на Асемблере , C++ , Delphi.А также командами на Unix и Linux.
fatum@xakep.ru

Все кто хочет переписываться. Вот моё мыло zmey1812@mail.ru



Ищу людей, которым знакома тематика хип-хоп, для работы над статьями на сайте Хипфэнс! Мылить на telefox@yandex.ru

мессадж можно закинуть на
board@xakep.ru

объявления рекламного харрактера не публикуются!!!

1. мы не будем рекламировать твою страничку, сервер и прочее
2. все письма с матом и прочей шнягой удаляются сразу
3. мы постараемся размещать сообщения в ближайших номерах, но ничего не обещаем :)

ИЗДАНИЯ

"Мобильные Компьютеры"
Мобильные компьютеры, коммуникаторы, смартфоны, ноутбуки, мобильная связь, цифровое фото. Тестирование и рекомендации.
www.mobilecomputers.ru

"Страна Игр"
Игры для PC, Sony PlayStation, Sony PlayStation2, Nintendo GameCube, Sega Dreamcast, GameBoy Advance, Онлайновые игры, компьютерное железо. Свежие новости, лучшие обзоры. Советы и тактика прохождения.
www.gameland.ru

"Хакер"
Взлом, интернет, компьютеры, новости и железо.
www.xakep.ru

"PlayStation"
Sony PlayStation, Sony PlayStation2. Новости, лучшие обзоры и тематические статьи. Коды, советы и прохождения лучших игр.
www.gameland.ru

ИНТЕРНЕТ ПРОЕКТЫ



www.e-shop.ru
Интернет-магазин компьютеров, видео игр и DVD



www.modernart.ru
"МодернАрт"
Магазин-галерея современного искусства

